KASPERSKY LAB

Kaspersky Mobile Security 7.0 Enterprise Edition

MANUAL DE UTILIZADOR

KASPERSKY MOBILE SECURITY 7.0 ENTERPRISE EDITION

Manual de Utilizador

© Kaspersky Lab
http://www.kaspersky.pt/

Data de Revisão: Agosto de 2009

Índice

CAPÍTULO 1. KASPERSKY MOBILE SECURITY 7.0 ENTERPRISE EDITION 5
1.1. Requisitos de hardware e software 6
1.2. Kit de Distribuição 6
1.3. Instalar o Kaspersky Mobile Security 6
1.3.1. Instalação através do computador do utilizador 7
1.3.2. Instalação através de uma mensagem SMS 8
1.4. Activar a aplicação 8

CAPÍTULO 2. KASPERSKY MOBILE SECURITY PARA SYMBIAN 9
2.1. Utilizar a aplicação 9
2.1.1. Iniciar a aplicação 9
2.1.2. Interface Gráfica do Utilizador 10
2.1.3. Configurações Gerais 11
2.1.4. Verificação e Protecção Anti-vírus 12
2.1.5. Utilizar a Quarentena 19
2.1.6. Utilizar o Anti-Spam 21
2.1.7. Utilizar o Anti-Roubo 27
2.1.8. Actualizar as bases da aplicação 31
2.1.9. Actualizar as configurações de funcionamento da aplicação 34
2.1.10. Utilizar o Módulo Firewall 35
2.1.11. Visualizar relatórios sobre o funcionamento da aplicação 36
2.2. Desinstalar a aplicação 37

CAPÍTULO 3. KASPERSKY MOBILE SECURITY PARA MICROSOFT WINDOWS MOBILE 40
3.1. Começar 40
3.1.1. Iniciar a aplicação 40
3.1.2. Interface Gráfica do Utilizador 41
3.2. Verificação anti-vírus e Protecção em Tempo Real 43
3.2.1. Verificação sob pedido 43
3.2.2. Protecção em Tempo Real 46
3.2.3. Verificação agendada 47

3.3. Utilizar a Quarentena 48
3.4. Utilizar os módulos Anti-Spam e Anti-Roubo 49
3.4.1. Módulo Anti-Spam 50
3.4.2. Separador Anti-Roubo 53
3.5. Actualizar as bases da aplicação 57
3.6. Actualizar as configurações de funcionamento da aplicação 59
3.7. Firewall 59
3.8. Visualizar relatórios sobre o funcionamento da aplicação 61
3.9. Desinstalar a aplicação 62

APÊNDICE A. KASPERSKY LAB 67

APÊNDICE B. CRYPTOEX LLC 69

APÊNDICE C. CONTRATO DE LICENCA DE UTILIZADOR FINAL DO KASPERSKY LAB 70

CAPÍTULO 1. KASPERSKY MOBILE SECURITY 7.0 ENTERPRISE EDITION

O **Kaspersky Mobile Security 7.0 Enterprise Edition** foi concebido para assegurar a protecção, face a programas maliciosos e mensagens de e-mail indesejadas, de dispositivos móveis com os sistemas operativos Symbian e Microsoft Windows Mobile e executa as seguintes funções:

- **protecção em tempo real** do sistema de ficheiros do dispositivo - intercepção e verificação de:
  - todos os objectos recebidos, transmitidos através de ligações sem fios (porta IV, Bluetooth) e mensagens SMS, durante a sincronização com o computador pessoal e ao transferir ficheiros através de um navegador;
  - ficheiros abertos no dispositivo móvel;
  - programas instalados a partir da interface do dispositivo.
- **verificação de objectos do sistema de ficheiros** do dispositivo móvel ou dos cartões de memória inseridos, a pedido do utilizador ou de acordo com o agendamento;
- **isolamento seguro face a objectos infectados** no armazenamento da quarentena;
- **actualização das bases do Kaspersky Mobile Security** utilizadas para verificar a existência de programas maliciosos e apagar objectos perigosos.
- **bloqueio de mensagens SMS indesejadas**.
- **bloqueio de acesso ou eliminação dos dados do utilizador** em caso de acções não-autorizadas com o dispositivo, como por exemplo em caso de roubo.
- **protecção do dispositivo móvel ao nível da rede**.

O utilizador pode usar as funcionalidades para o controlo flexível das configurações de funcionamento Kaspersky Anti-Virus, visualizar o actual estado da protecção anti-vírus e o log de eventos no qual são registadas as acções da aplicação.

A aplicação inclui um sistema de menus e uma interface de utilizador intuitiva e fácil de utilizar.

Nota

Ao detectar um programa malicioso, o Kaspersky Mobile Security pode desinfectar o objecto infectado (se a desinfecção for possível), apagá-lo ou colocá-lo na quarentena. A aplicação não guarda cópias de segurança dos objectos que foram apagados.

1.1. Requisitos de hardware e software

O Kaspersky Mobile Security foi concebido para ser instalado em dispositivos móveis com um dos seguintes sistemas operativos:

- Symbian OS 9.1, 9.2 Series 60 UI.
- Microsoft Windows Mobile 5.0.
- Microsoft Windows Mobile 6.0.

1.2. Kit de Distribuição

Você pode adquirir o Kaspersky Mobile Security pela Internet (o pacote da aplicação e respectiva documentação em formato electrónico). O Kaspersky Mobile Security também pode ser adquirido em lojas de serviços de comunicações móveis. Para mais detalhes, contacte o seu operador de comunicações móveis.

1.3. Instalar o Kaspersky Mobile Security

Nota

O Kaspersky Mobile Security instalado não é adequado para cópia de segurança e restauro.

A aplicação é instalada através de uma instalação centralizada a partir do Kaspersky Administration Kit. O Administrador de Rede pode utilizar um dos dois métodos de instalação da aplicação.

- Instalação através do computador do utilizador;
- Instalação através de uma mensagem SMS.

Para mais detalhes sobre a instalação remota da aplicação, consulte o "Manual de Administrador" do Kaspersky Mobile Security 7.0 Enterprise Edition.

1.3.1. Instalação através do computador do utilizador

Depois de ligar o dispositivo móvel a um computador incluído na rede lógica do Servidor de Administração, abrir-se-á a janela do utilitário *kmlisten.exe* (ver Figura 1). Este utilitário foi concebido para assegurar a instalação do Kaspersky Mobile Security 7.0 Enterprise Edition num dispositivo móvel.

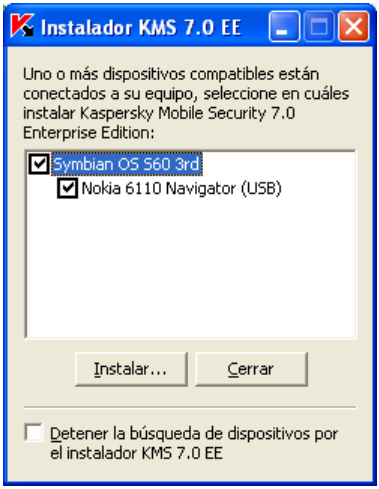
Instalador KMS 7.0 EE
Uno o más dispositivos compatibles están conectados a su equipo, seleccione en cuáles instalar Kaspersky Mobile Security 7.0 Enterprise Edition:
Symbian OS S60 3rd
Nokia 6110 Navigator (USB)
Instalar...
Cerrar
Detener la búsqueda de dispositivos por el instalador KMS 7.0 EE

Figura 1. Utilitário **Kmlisten**

Para instalar o Kaspersky Mobile Security, execute as seguintes acções:

Através da janela do utilitário *kmlisten.exe*, assinale a caixa junto ao nome do dispositivo no qual deseja instalar a aplicação e clique no botão **Instalar**. O kit de distribuição para a instalação da aplicação será copiado para o seu dispositivo móvel e iniciado.

1.3.2. Instalação através de uma mensagem SMS

Para instalar a aplicação, o administrador de rede pode utilizar o serviço de instalação através de uma mensagem SMS (para mais detalhes consulte o Manual de Administrador do Kaspersky Mobile Security 7.0 Enterprise Edition). Será enviada para o dispositivo móvel uma mensagem SMS que contém o URL do servidor no qual está localizado o kit de instalação da aplicação.

Para instalar a aplicação através de uma mensagem SMS, execute as seguintes acções:

1. Abra um SMS com o URL do servidor a partir do qual será transferido o pacote de instalação do Kaspersky Mobile Security.
2. Utilize o link contido na mensagem de texto para transferir o kit de instalação da aplicação para o dispositivo.
3. Guarde o kit de instalação da aplicação.

O processo de instalação da aplicação irá então iniciar-se automaticamente.

1.4. Activar a aplicação

Nota

É necessária a activação da aplicação, caso contrário as funcionalidades da aplicação não estarão disponíveis.

A activação do Kaspersky Mobile Security 7.0 Enterprise Edition é efectuada durante a sincronização com o Servidor de Administração. Durante a sincronização, é copiado para dispositivo o ficheiro de chave especificado durante a criação da política para dispositivos móveis (para mais detalhes sobre as políticas para dispositivos móveis do Kaspersky Administration Kit, consulte o Manual de Administrador do Kaspersky Mobile Security 7.0 Enterprise Edition).

O processo de sincronização da aplicação com o serviço de Administração será automaticamente iniciado com o intervalo especificado na política para dispositivos móveis. Também pode iniciar, manualmente, o processo de sincronização (ver secção 2.1.9 na página 34 ou na secção 3.6 na página 59).

Nota

Enquanto a política estiver a ser criada, deve ser bloqueada a possibilidade de alteração do ficheiro de chave do dispositivo móvel. Caso contrário, o dispositivo não será activado durante a sincronização com o Servidor de Administração.

CAPÍTULO 2. KASPERSKY MOBILE SECURITY PARA SYMBIAN

Este capítulo contém a descrição do funcionamento do Kaspersky Mobile Security 7.0 para dispositivos com os sistemas operativos Symbian versão 9.1, 9.2 ou Series 60 UI.

2.1. Utilizar a aplicação

Esta secção contém informação sobre a configuração das verificações anti-vírus, da protecção em tempo real, da filtragem de mensagens SMS e MMS, da verificação anti-vírus do dispositivo, da actualização das bases, das definições de funcionamento da aplicação e da protecção do dispositivo ao nível da rede, etc.

2.1.1. Iniciar a aplicação

Para iniciar o Kaspersky Mobile Security, execute as seguintes acções:

1. Abra o menu principal do dispositivo.
2. Seleccionar o **KMS 7.0 EE** e inicie a aplicação, utilizando o item **Abrir** do menu **Opções**.

Após a inicialização do dispositivo, no ecrã do mesmo será exibida uma janela com as principais componentes do Kaspersky Mobile Security (ver Figura 2).

- **Prot. em Tempo Real** - utilização do modo de protecção em tempo real (ver secção 2.1.4 na página 12);
- **Última Verif. Completa** – data da última verificação anti-vírus do dispositivo.
- **Data da Base de Dados –** data de distribuição da base de dados anti-vírus utilizada pela aplicação.
- **Config. do Anti-Spam** – modo de funcionamento do Anti-Spam (ver secção 2.1.6 na página 21).

- **Nível da Firewall** – nível de protecção ao nível da rede (ver secção 2.1.9 na página 34).

Figura 2. Janela de estado das componentes da aplicação

Para aceder à interface da aplicação, clique em **OK**.

2.1.2. Interface Gráfica do Utilizador

A Interface Gráfica do Utilizador (GUI) contém seis separadores:

- Ao utilizar o separador **Verificação**, pode executar uma verificação anti-vírus do dispositivo, editar as configurações da verificação anti-vírus, da protecção em tempo real e da quarentena e configurar o agendamento para a verificação automática.
- Ao utilizar o separador **Actualização**, pode actualizar a base de dados anti-vírus, editar as configurações de actualização e configurar o agendamento para a actualização.
- Ao utilizar o separador **Firewall**, pode monitorizar as actividades de rede e proteger o dispositivo ao nível da rede.
- O separador **Anti-Roubo** permite-lhe bloquear o dispositivo e apagar informações do mesmo em caso de roubo ou perda do dispositivo (módulo Anti-Roubo).
- Ao utilizar o separador **Anti-Spam,** pode configurar a filtragem de mensagens SMS recebidas (módulo Anti-Spam).

- Ao utilizar o separador **Informações**, pode visualizar os registos sobre o funcionamento das componentes da aplicação, informação geral sobre a aplicação e as bases anti-vírus utilizadas e editar as configurações gerais utilizadas no funcionamento da aplicação.

Para navegar entre os separadores, utilize o joystick do dispositivo ou seleccione o item **Abrir Página** no menu **Opções** (ver Figura 3).

Figura 3. Menu **Opções**

Para voltar à janela de estado das componentes da aplicação, seleccione o item **Estado Actual** no menu **Opções**.

2.1.3. Configurações Gerais

Através das configurações do separador **Informações** no item **Configurações** (ver Figura 4), você pode configurar as seguintes funções da aplicação:

- **Mostrar Ecrã de Estado** determina se o estado actual será exibido com o arranque da aplicação.
- **Tamanho do Log** determina o tamanho máximo do log. Quando o valor mínimo do limite especificado for atingido, as mensagens antigas do log serão apagadas até que o valor máximo do limite especificado seja atingido.
- **Luz de Fundo** determina se o ecrã está ou não iluminado durante a verificação anti-vírus. Por defeito, a opção da luz de fundo está desactivada.

- **Reproduzir Som** controla a utilização de notificações sonoras em caso de determinados eventos (detecção de objectos infectados, mensagem acerca do estado da aplicação, etc.). Por defeito, a reprodução do sinal sonoro em caso de detecção de vírus depende do perfil de dispositivo (o valor da configuração **Dependente do perfil**). Seleccione **Activado**, se desejar utilizar a notificação sonora, independentemente do perfil de dispositivo seleccionado.
- **Volume do som** determina o volume da reprodução da notificação sonora quando for detectado um objecto infectado.
- **Vibração** determina se o dispositivo irá vibrar quando for detectado um objecto infectado. Por defeito, a vibração está activada.

Figura 4. Menu **Configurações**

Para editar os valores das configurações , utilize o joystick do dispositivo ou seleccione o item **Alterar** no menu **Opções**.

2.1.4. Verificação e Protecção Anti-vírus

Através do separador **Verificação**, você pode executar uma verificação anti-vírus de todo o sistema de ficheiros e da memória do dispositivo ou de uma pasta ou ficheiro individual. Também pode alterar as configurações da verificação anti-vírus e da protecção anti-vírus em tempo real, visualizar o relatório sobre os resultados da verificação e criar o agendamento para o início automático da verificação.

2.1.4.1. Protecção em tempo real e verificação sob pedido

A protecção em tempo real é o modo de funcionamento no qual a parte residente do Kaspersky Mobile Security permanece sempre na RAM (memória de acesso aleatório) do dispositivo e monitoriza todos os dados, incluindo os dados recebidos pelo dispositivo.

A protecção em tempo real é iniciada desde o momento em que o dispositivo é ligado e continua activa até este ser desligado (a não ser que este modo seja desactivado nas configurações de protecção).

O Kaspersky Mobile Security também permite efectuar uma verificação completa do sistema de ficheiros do dispositivo, incluindo a análise dos objectos existentes nos cartões de memória inseridos no dispositivo.

Os resultados da protecção em tempo real e da verificação sob pedido serão registados no relatório. Para visualizar o relatório, seleccione o item **Relatórios** no separador **Verificação**.

Para iniciar a protecção em tempo real:

1. Seleccione o item **Configurações** no separador **Verificação**.
2. Seleccione **Configurações de protecção** na secção **Configurações**.
3. Active / desactive o modo de protecção em tempo real, definindo o valor correspondente para a configuração **Prot. em Tempo Real**.

Para alterar as configurações de funcionamento da protecção em tempo real:

1. Seleccione o item **Configurações** no separador **Verificação**.
2. Seleccione **Configurações de protecção** na secção **Configurações**.
3. Defina a área de verificação na secção **Máscara de Verificação**, seleccionando os tipos de ficheiros a verificar:
   - **Todos os ficheiros** – verificar todos os ficheiros.
   - **Ficheiros executáveis** – verificar apenas ficheiros de programas executáveis (por exemplo *.exe, *.sis, *.mdl, *.app).
4. Determine a acção a executar quando for detectado um objecto infectado (a configuração **Acção ao Detectar Vírus**).

   Por defeito, os objectos de software malicioso detectados são colocados na quarentena (valor de configuração **Quarentena**).

Para garantir que a informação sobre a detecção de um objecto infectado é registada no relatório da aplicação, seleccione o valor **Log do evento**.

Para fazer com que a aplicação elimine os objectos de software malicioso detectados, sem solicitar ao utilizador a acção a executar, seleccione o valor **Elimin. Automática**.

5. Active / desactive o modo de verificação de cartões novos (a configuração **Verificar Novo Cartão**).

   Por defeito, se for detectado um cartão de memória, a aplicação notifica que o cartão deve ser verificado.

   Para activar a verificação de cartões de memória ligados ao dispositivo, defina o valor **Verific. Automática**. Para desactivar a verificação de cartões de memória, seleccione **Desactivar**.

6. Active / desactive a apresentação do ícone de protecção (a configuração **Mostrar Ícone no Ecrã**).

   Se deseja que o ícone da aplicação seja sempre exibido no ecrã do dispositivo quando a protecção em tempo real estiver activada, seleccione o valor **Sempre** no item correspondente do menu. Se deseja que o ícone seja exibido apenas no menu do dispositivo, seleccione **Apenas no Menu**. Se não deseja que este ícone seja exibido, seleccione **Off**.

Para alterar as configurações de funcionamento da verificação sob pedido:

1. Seleccione o item **Configurações** no separador **Verificação**.
2. Seleccione **Configurações de verificação** na secção **Configurações**.
3. Defina a área de verificação na secção **Máscara de Verificação**, seleccionando os tipos de ficheiros a verificar:

   - **Todos os ficheiros** – verificar todos os ficheiros.
   - **Ficheiros executáveis** – verificar apenas ficheiros de programas executáveis (por exemplo *.exe, *.sis, *.mdl, *.app).

4. Determine a acção a executar quando for detectado um objecto infectado (a configuração **Acção ao Detectar Vírus**).

   Por defeito, a aplicação tenta desinfectar os objectos de software malicioso detectados (valor de configuração **Tentar desinfectar**).

   Para colocar na quarentena os objectos de software malicioso detectados, seleccione o valor **Quarentena**.

Para garantir que a informação sobre a detecção de um objecto infectado é registada no relatório da aplicação, seleccione o valor **Log do evento**.

Para fazer com que a aplicação elimine os objectos de software malicioso detectados, sem perguntar ao utilizador a acção a executar, seleccione o valor **Elimin. Automática**.

Para garantir que é aberta uma notificação a solicitar ao utilizador a acção a executar quando for detectado um objecto infectado, seleccione o valor **Perguntar ao Utiliz.**.

5. Especifique uma acção a executar caso a desinfecção de um objecto infectado não seja possível (a configuração **Se a desinfecção falhar**).

   Por defeito, os objectos de software malicioso detectados são colocados na quarentena (valor de configuração **Quarentena**).

   Para garantir que a informação sobre a detecção de um objecto infectado é registada no relatório da aplicação, seleccione o valor **Log do evento**.

   Para fazer com que a aplicação elimine os objectos de software malicioso detectados, sem perguntar ao utilizador a acção a executar, seleccione o valor **Elimin. Automática**.

   Para garantir que é aberta uma notificação a solicitar ao utilizador a acção a executar quando for detectado um objecto infectado, seleccione o valor **Perguntar ao Utiliz.**.

6. Active / desactive a verificação da memória ROM do dispositivo (a configuração **Verificar ROM**).

   Nalguns casos, a memória ROM (memória apenas de leitura) pode-se tornar vulnerável aos programas maliciosos. Para permitir a verificação da memória ROM pelo Kaspersky Mobile Security, seleccione o valor **Sim**.

7. Active / desactive a descompactação de arquivos SIS e ZIP (a configuração **Descompactar arquivos**).

   Se deseja que a aplicação execute a descompactação de arquivos SIS e ZIP, seleccione **Sim**. Se os arquivos não precisarem de ser descompactados durante a verificação, seleccione **Não**.

Nota

Para editar os valores das configurações, utilize o joystick do dispositivo ou seleccione o item **Alterar** no menu **Opções**.

Por defeito, a aplicação utiliza os valores das configurações recomendadas pelos especialistas da Kaspersky Lab. Se deseja voltar às configurações recomendadas enquanto estiver a utilizar a aplicação, abra o separador **Verificação** e seleccione o item **Predefinições** a partir do menu **Opções**.

Para iniciar uma verificação anti-vírus, execute as seguintes acções:

1. Inicie o Kaspersky Mobile Security (ver secção 2.1.1 na página 9).
2. Através do separador **Verificação** (ver Figura 5) seleccione o item **Verificar Tudo**, se desejar verificar todo o sistema de ficheiros do dispositivo ou **Verificar Pasta**, se desejar verificar uma pasta individual.

Figura 5. Separador **Verificação**

Se tiver seleccionado o item **Verificar Pasta**, abrir-se-á uma janela que apresenta o sistema de ficheiros do dispositivo. Para navegar ao longo do sistema de ficheiros, utilize os botões do joystick do seu dispositivo. Para verificar uma pasta, mova o cursor para a pasta que deseja verificar e seleccione o item **Iniciar Verificação** a partir do menu **Opções**.

Depois de a verificação começar, abrir-se-á a janela de progresso da verificação, na qual será apresentado o actual estado da tarefa: o número de objectos verificados, o caminho para o objecto que está a ser verificado naquele momento e o indicador de percentagem de progresso (ver Figura 6).

Figura 6. Janela **Progresso da Verificação**

Se for detectado um objecto infectado, será executada a acção especificada pela respectiva configuração na secção **Configurações→Configurações de verificação**.

Figura 7. Notificação sobre a detecção de vírus

Depois de a verificação estar concluída, serão apresentadas as estatísticas gerais sobre os objectos maliciosos detectados e apagados.

Para desactivar a luz de fundo do ecrã durante a verificação,

Aceda ao separador **Informações**, abra o menu **Configurações** e seleccione o valor **Sim** para a configuração **Luz de Fundo**.

Por defeito, a luz de fundo desligar-se-á automaticamente para poupar o tempo de vida da bateria.

2.1.4.2. Verificação agendada

O Kaspersky Mobile Security permite ao utilizador criar um agendamento para a verificação automática do dispositivo. A verificação é executada em segundo plano. Ao detectar um objecto infectado, a acção especificada nas configurações de verificação será executada com esse objecto (ver secção 2.1.4.1 na página 13).

Por defeito, a verificação agendada está desactivada.

Figura 8. Menu **Agendamento**

Para criar o agendamento de inicialização da verificação:

Seleccione o item **Agendamento** no separador **Verificação** e especifique as configurações da **Verif. Autom.** (ver Figura 8):

- **Diariamente** – a verificação será efectuada todos os dias. Especifique a **Hora da Verif. Autom.** no campo de registo.

- **Semanalmente** - a verificação será efectuada uma vez por semana. Especifique o **Dia da Verif. Autom.** e a **Hora da Verif. Autom.**.

2.1.5. Utilizar a Quarentena

Os objectos infectados colocados na quarentena não representam qualquer ameaça para o dispositivo e podem ser apagados ou restaurados mais tarde.

A aplicação pode colocar os objectos infectados na quarentena, automaticamente ou após a sua confirmação.

Se deseja que a aplicação coloque os objectos de software malicioso detectados, automaticamente, na quarentena sem perguntar ao utilizador:

1. Abra o separador **Verificação**.
2. Seleccione o item **Configurações**.
3. Seleccione o item **Configurações de verificação** ou **Configurações de protecção**.
4. Seleccione **Quarentena** como o valor para a configuração **Acção ao Detectar Virus**.

Se seleccionou **Perguntar ao Utiliz.** como a acção a executar, então quando for detectado um objecto infectado, o Kaspersky Mobile Security dar-lhe-á a opção de apagar este objecto ou de o colocar na quarentena.

Para ver a lista de objectos em quarentena:

Abra o separador **Verificação** e seleccione o item **Quarentena** (ver Figura 9).

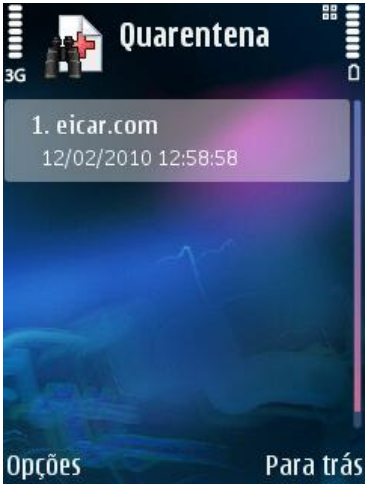

Figura 9. Objectos infectados em quarentena

O menu **Opções**, acessível a partir da janela de visualização da quarentena, permite ao utilizador:

- Ver informação detalhada sobre cada objecto da quarentena (**Ver Detalhes**).
- Apagar o objecto seleccionado (**Remover ficheiro**).
- Limpar a quarentena, apagando todos os objectos em quarentena (**Remover todos**).
- Restaurar o objecto da Quarentena para a sua pasta original (**Restaurar ficheiro**).
- Visualizar a ajuda sobre a Quarentena (**Ajuda**).

Para definir as configurações da quarentena:

1. Abra o separador **Verificação**.
2. Seleccione o item **Configurações**.
3. Seleccione o separador **Quarentena** (ver Figura 10).

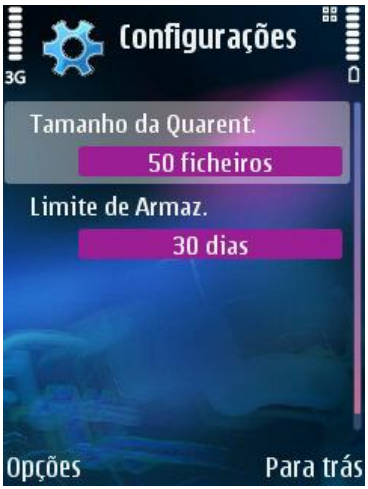

Figura 10. Configurações da Quarentena

A configuração **Tamanho da Quarent.** determina o número máximo de objectos infectados que podem ser armazenados na quarentena. Os valores permitidos são **20**, **50** ou **100** ficheiros.

A configuração **Limite de Armaz.** determina o período de tempo durante o qual os objectos infectados podem estar armazenados na quarentena. Depois de esse período expirar, os objectos infectados serão automaticamente apagados.

Nota

Para restaurar os valores das configurações da quarentena recomendadas pelos especialistas da Kaspersky Lab, seleccione **Predefinições** a partir do menu **Opções**.

2.1.6. Utilizar o Anti-Spam

O módulo Anti-Spam foi concebido para assegurar a protecção do seu dispositivo contra mensagens SMS indesejadas.

A filtragem baseia-se na utilização das listas "negra" e "branca". Estas listas contêm números de telefone e exemplos de frases características de mensagens spam e não-spam. A análise de mensagens será efectuada pela seguinte ordem:

- verificar se o número do remetente está incluído na lista "negra";
- verificar se o número do remetente está incluído na lista "branca";

- verificação do texto da mensagem quanto à presença de frases existentes na lista “negra”;
- verificação do texto da mensagem quanto à presença de frases existentes na lista “branca”;

Se for detectada pelo menos uma correspondência, a verificação será interrompida. A mensagem que contenha um elemento existente na lista “negra” será bloqueada. A mensagem que contenha um elemento existente na lista “branca” será permitida.

2.1.6.1. Modos de funcionamento do Anti-Spam

O Anti-Spam filtra mensagens de acordo com um dos seguintes modos:

- **Activar.** Neste modo, o Anti-Spam filtra as mensagens recebidas através das listas "negra" e "branca". Quando for recebida uma mensagem de um número de telefone não incluído em nenhuma das listas, o Anti-Spam notificará o utilizador e dar-lhe-á a opção de bloquear ou permitir a recepção da mensagem e ainda a opção de adicionar este número de telefone à lista "branca" ou "negra".
- **Lista Negra.** Neste modo, o Anti-Spam bloqueia a recepção das mensagens que correspondam aos critérios da “lista negra". Todas as outras mensagens serão permitidas.
- **Lista Branca.** Neste modo, o Anti-Spam permite as mensagens que correspondam aos critérios da “lista branca". Todas as outras mensagens serão bloqueadas.
- **Desactivar.** Neste modo, o Anti-Spam está desactivado. Não é efectuada a filtragem das mensagens recebidas.

Para seleccionar o modo de funcionamento do Anti-Spam:

1. Abra o separador **Anti-Spam**.
2. Seleccione o item **Configurações**.
3. Defina o modo de funcionamento, através da configuração **Config. Anti-Spam**.

2.1.6.2. Editar as listas “negra” e “branca”

As listas **"Negra"** e **"Branca"** contêm registos com números de telefone, cujas mensagens SMS serão bloqueadas ou permitidas pelo Anti-Spam. A informação sobre as mensagens bloqueadas ou apagadas será registada na secção **Relatórios**.

Nota

As mensagens não incluídas em nenhumas das listas não serão bloqueadas!

Para inserir alterações na lista "negra" ou "branca",

abra o separador **Anti-Spam** e seleccione o item correspondente (ver Figura 11).

Para editar a lista, utilize o menu **Opções**:

- **Adicionar Registo** – adicionar um novo registo à lista.
- **Editar Registo** – editar o registo actual.
- **Remover Registo** – apagar o registo da lista.
- **Remover Todos** – limpar a lista, apagando todos os registos.
- **Ajuda** – obter Ajuda sobre como gerir a lista.

Figura 11. Separador **Anti-Spam**

Quando selecciona o item **Adicionar registo** ou **Editar registo**, será necessário especificar os seguintes parâmetros do registo (ver Figura 12).

- **Número de telefone**. Especifique o número de telefone para o qual a recepção de mensagens será bloqueada ou permitida. Este número pode começar com um dígito ou um "+" e tem de conter unicamente dígitos. Para além disso, ao especificar um número, você pode utilizar as máscaras "?" e "*".

- **Texto**. Especifique o texto, cuja detecção na mensagem recebida fará com que essa mensagem seja permitida ou bloqueada.

Figura 12. Lista Negra

2.1.6.3. Configurações de funcionamento do Anti-Spam

Para editar as configurações do Anti-Spam:

abra o separador **Anti-Spam** e seleccione o item **Configurações** (ver Figura 13).

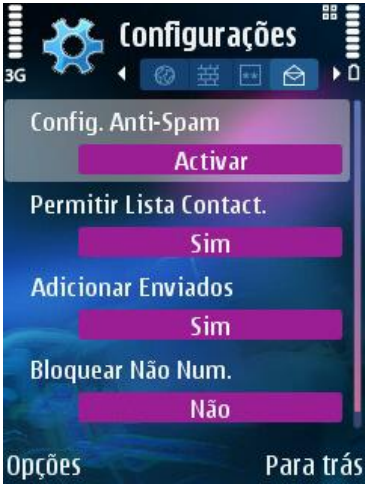

Figura 13. Configurações do Anti-Spam

No menu **Configurações** estão disponíveis as seguintes configurações do Anti-Spam:

- **Config. Anti-Spam** – Modo de funcionamento do Anti-Spam (ver secção 2.1.6.1 na página 22).
- **Permitir Lista Contact.** Se esta configuração tiver atribuído o valor **Sim**, o Anti-Spam não bloqueará a recepção de mensagens dos números de telefone incluídos na sua lista de contactos. Se esta opção estiver desactivada (valor **Não**), o Anti-Spam irá efectuar a filtragem, dependendo se o número de telefone estiver incluído na lista "negra" ou na lista "branca".
- **Adicionar Enviados**. Se esta configuração tiver atribuído o valor **Sim**, todos os números de telefone, para os quais você enviar mensagens SMS, serão automaticamente adicionados à lista "branca". Para desactivar esta opção, seleccione **Não**.
- **Bloquear Não Num.** Se esta configuração tiver atribuído o valor **Não**, o Anti-Spam não bloqueará todas as mensagens recebidas de números não numéricos. Para activar esta opção, seleccione **Sim**.

Nota

Esta configuração apenas afectará os registos criados pelo Anti-Spam nas seguintes situações:

- ao adicionar à lista "branca" os números usados em mensagens enviadas (configuração **Adicionar enviados** está activada);
- ao adicionar, a uma das listas, novos números de telefone, a partir dos quais são recebidas mensagens (ver secção 2.1.6.4 na página 26).

Para editar os valores das configurações, utilize o joystick do dispositivo ou seleccione o item **Alterar** no menu **Opções**.

2.1.6.4. Acções a executar em relação às mensagens

Quando receber uma mensagem SMS ou MMS de um número de telefone não incluído nas listas "negra" ou "branca", essa mensagem será interceptada pelo Anti-Spam e será exibida uma notificação no ecrã do dispositivo (ver Figura 14)

Através do menu **Opções**, pode seleccionar uma das seguintes acções a serem executadas com a mensagem:

- **Adicionar à Lista Branca** – permite a recepção da mensagem e adiciona o número de telefone do remetente à lista "branca".
- **Adicionar à Lista Negra** – bloqueia a recepção da mensagem e adiciona o número de telefone do remetente à lista "negra".
- **Ignorar** – permite a recepção da mensagem. Neste caso, o número de telefone do remetente não será adicionado a nenhuma das listas.

A informação sobre as mensagens bloqueadas será registada nos relatórios da aplicação. Para visualizar o relatório, seleccione o item **Relatórios** no separador **Anti-Spam**.

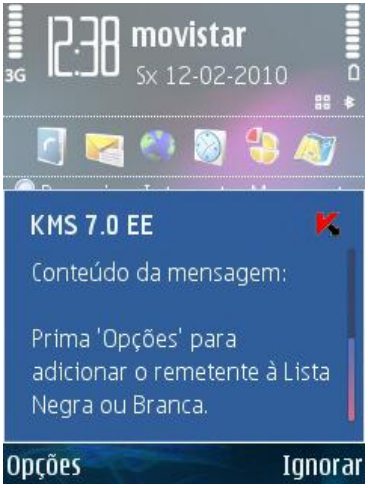

Figura 14. Aviso do Anti-Spam

2.1.7. Utilizar o Anti-Roubo

Este módulo foi concebido para garantir a protecção dos dados armazenados no dispositivo móvel contra o acesso não-autorizado, no caso de o dispositivo ser roubado ou perdido.

Quando aceder às configurações do módulo pela primeira vez, terá de definir uma password. Mais tarde esta password é utilizada para aceder às configurações do módulo e gerir as respectivas funções. Função **Bloqueio por SMS** – permite bloquear o dispositivo por ordem do utilizador. Você pode desbloquear o dispositivo apenas depois de inserir uma password utilizada para aceder ao módulo Anti-Roubo. Para desbloquear o dispositivo através da função Bloqueio por SMS, envie uma mensagem SMS com o texto: "`block:code`" para o dispositivo. Por defeito, a função Bloqueio por SMS está desactivada. Para activar a função, seleccione **On**.

A **Limpeza por SMS** permite apagar dados pessoais do utilizador (contactos, mensagens, dados do cartão de memória, configurações de rede). Para utilizar a função Limpeza por SMS, envie uma mensagem SMS com o texto: "`clean:code`" para o dispositivo. Por defeito, a função Limpeza por SMS está desactivada. Para activar a função, seleccione **On**.

Protecção do Cartão SIM – permite enviar para os números especificados um novo número de telefone e assim bloquear o dispositivo, caso o cartão SIM seja substituído nesse dispositivo roubado. Para activar a função, seleccione **On**.

Se for necessário alterar a password utilizada para trabalhar com o módulo Anti-Roubo, seleccione o item **Alterar password**. Insira a nova password e a respectiva confirmação e prima o botão **OK**.

Cada vez que aceder às configurações do Módulo Anti-Roubo (ver Figura 14), você terá de inserir a password que definiu anteriormente.

Figura 15. Separador **Anti-Roubo**

A informação sobre o funcionamento do módulo será registada nos relatórios da aplicação. Para visualizar o relatório, seleccione o item **Relatórios** no separador **Anti-Roubo**.

2.1.7.1. Secção Limpeza por SMS

Para configurar as definições de funcionamento da função Limpeza por SMS:

1. Abra o separador **Anti-Roubo** e insira a password (ver secção 2.1.7 na página 27).
2. Seleccione o item **Configurações**.
3. Seleccione o item **Limpeza por SMS**.

A secção **Limpeza por SMS** contém a lista de dados que podem ser seleccionados para eliminação caso o seu dispositivo seja perdido (ver Figura 16).

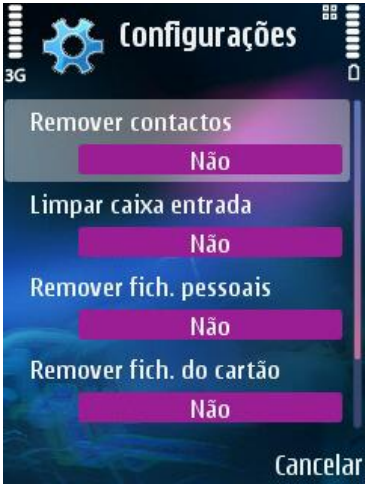

Figura 16. Separador **Limpeza por SMS**

Se deseja poder apagar a lista de contactos, caso o seu dispositivo móvel seja roubado ou perdido, seleccione o item **Remover contactos** e atribua-lhe o valor **Sim**.

Nota

Apenas serão apagados os contactos da lista de contactos guardada no dispositivo. A lista de contactos do cartão SIM não será apagada.

Para apagar e-mails, mensagens SMS (pastas Caixa de Entrada e Caixa de E-mail), seleccione o item **Limpar caixa entrada** e atribua-lhe o valor **Sim**.

O item **Remover fich. pessoais** assegura a eliminação dos dados pessoais (dados da pasta C:\Data\). Por defeito, a eliminação dos ficheiros pessoais não está activada. Se deseja poder apagar os seus dados pessoais, caso o seu dispositivo seja roubado ou perdido, seleccione este item e atribua-lhe o valor **Sim**.

Utilize o item **Remover fich. do cartão** para activar a limpeza do cartão de memória do dispositivo perdido. Por defeito, esta função está desactivada. Para activar a eliminação de dados do cartão de memória, seleccione **Remover fich. do cartão** e seleccione o valor **Sim**.

Para activar a opção de eliminação das configurações da ligação de rede, seleccione o item **Remover conf. de rede** e defina o valor para **Sim**.

Prima o botão **OK** para guardar as alterações.

2.1.7.2. Configurações da Protecção do Cartão SIM

Para configurar as definições da **Protecção do Cartão SIM**, aceda ao separador **Anti-Roubo**. Insira a password (ver secção 2.1.7 na página 27) e depois seleccione **Protecção do Cartão SIM** na janela que se abre.

A secção **Protecção do Cartão SIM** foi concebida para monitorizar a substituição do cartão SIM no dispositivo (ver Figura 17).

Figura 17. Separador **Protecção do Cartão SIM**

Nos campos **Nº de telefone 1** e **Nº de telefone 2** insira os números de telefone para os quais gostaria de receber um novo número de telefone se o cartão SIM for substituído no seu dispositivo. Estes números podem começar com um dígito ou um "+" e têm de conter unicamente dígitos.

Para além disso, você pode activar o bloqueio do seu dispositivo para o caso em que o cartão SIM seja substituído. Para o fazer, seleccione o item **Bloquear dispositivo** e atribua-lhe o valor **Sim**. Você pode desbloquear o dispositivo ao inserir a password definida para aceder ao módulo Anti-Roubo. Por defeito, o bloqueio do dispositivo está desactivado.

Prima o botão **OK** para guardar as alterações que efectuou.

2.1.8. Actualizar as bases da aplicação

A verificação de programas maliciosos é executada com base nos registos das bases da aplicação, que contêm a descrição de todos os programas maliciosos actualmente conhecidos. Por essa razão, é extremamente importante manter as suas bases actualizadas.

Você pode actualizar as bases manualmente ou de acordo com um agendamento. As actualizações são efectuadas a partir dos servidores de actualização da Kaspersky Lab, através da Internet.

Você pode activar a verificação automática do seu dispositivo após cada actualização das bases do Kaspersky Mobile Security. Para o fazer, aceda ao item **Configurações** no separador **Actualização** e atribua o valor **On** ao item **Verif. após Actualiz.**.

O valor da configuração **Verif. Quar. ao Actualiz.** determina se os objectos da quarentena serão reanalisados cada vez que as bases da aplicação forem actualizadas. Por defeito, essa verificação é executada. Se não desejar que essa verificação seja executada, seleccione **Off**.

Se for necessário alterar o ponto de acesso activo, utilize a configuração **Ponto de Acesso**. Depois seleccione o valor desejado na lista. Por defeito, o ponto de acesso é o ponto predefinido do dispositivo.

O valor da configuração **Servidor de Actualiz.** determina a origem de actualização das bases da aplicação: os servidores de actualização da Kaspersky Lab (valor **Usar predefinido**) ou um outro servidor especificado pelo utilizador (valor **Definido pelo Utiliz.**). Se tiver seleccionado o valor **Definido pelo Utiliz.**, insira o URL na janela que se abre. Se necessário, pode especificar um servidor de actualização alternativo.

Pode ver informação detalhada sobre as bases utilizadas no item **Inform. da BD** do separador **Informações**.

A informação sobre a actualização das bases será registada nos relatórios da aplicação. Para visualizar o relatório, seleccione o item **Relatórios** no separador **Actualização**.

2.1.8.1. Configurações de Actualização

Para configurar as actualizações das bases da aplicação, execute as seguintes acções:

1. Inicie o Kaspersky Mobile Security (ver secção 2.1.1 na página 9).
2. Aceda ao item **Configurações** no separador **Actualização** (ver Figura 18).

Figura 18. Separador **Actualização**

3. Seleccione o ponto de acesso (a configuração **Ponto de Acesso**) (ver Figura 19).

> **Nota**
>
> O ponto de acesso é configurado através das definições fornecidas pelo seu fornecedor de Internet sem fios.

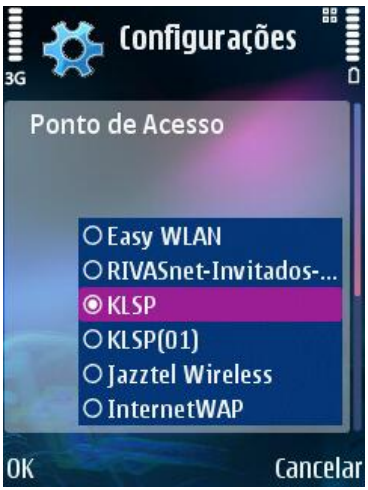

Figura 19. Seleccionar o ponto de acesso

4. Se necessário, insira o endereço do servidor de actualização. Para o fazer, seleccione o item **Servidor de Actualiz.** e depois seleccione a opção **Definido pelo Utiliz**. Insira o URL da origem de actualização na janela que se abre (ver Figura 20).

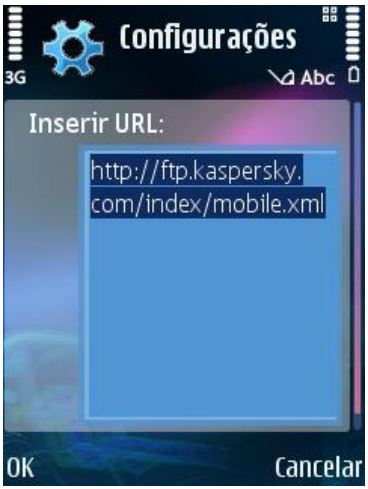

Figura 20. Endereço do servidor de actualização

Por defeito, as actualizações são efectuadas a partir do servidor de actualização da Kaspersky Lab: http://ftp.kaspersky.com/index/mobile.xml.

Nota!

Independentemente de a ligação à Internet ter sido aberta anteriormente, esta será interrompida depois de a actualização estar concluída.

2.1.8.2. Actualização manual

Para iniciar uma actualização manual das bases de dados anti-vírus:

1. Inicie o Kaspersky Mobile Security (ver secção 2.1.1 na página 9).
2. Seleccione o item **Actualização** no separador **Actualização** (ver Figura 18)

2.1.8.3. Actualização Agendada

Para criar um agendamento para a inicialização da actualização das bases da aplicação:

1. Inicie o Kaspersky Mobile Security (ver secção 2.1.1 na página 9).
2. Seleccione o item **Agendamento** no separador **Actualização** e configure as definições da **Actualização Autom.**:
   - **Off** – para não efectuar actualizações agendadas.
   - **Diariamente** - a actualização será efectuada todos os dias. Especifique a hora da actualização no campo correspondente.
   - **Semanalmente** - a actualização será efectuada uma vez por semana. Especifique o dia e a hora da actualização nos campos correspondentes.

2.1.9. Actualizar as configurações de funcionamento da aplicação

Nota

Para mais detalhes sobre o funcionamento conjunto do Kaspersky Mobile Security e do Kaspersky Administration Kit, consulte o Manual de Administrador do Kaspersky Mobile Security.

Ao utilizar o Kaspersky Mobile Security juntamente com o Kaspersky Administration Kit, as configurações de funcionamento da aplicação serão definidas pela política para um grupo de dispositivos móveis. A activação da aplicação e a implementação das configurações da política bloqueadas para impedir alterações irão ocorrer quando um dispositivo for adicionado ao grupo de administração.

Mais tarde, a sincronização da aplicação com o Servidor de Administração será, automaticamente, executada em intervalos definidos nas configurações da política.

Para iniciar a sincronização manual da aplicação com o Servidor de Administração:

1. Inicie o Kaspersky Mobile Security (ver secção 2.1.1 na página 9).
2. Abra o separador **Actualização**.
3. Seleccione o item **Sincronização**.

Durante a sincronização, as configurações de funcionamento da aplicação serão carregadas a partir do Servidor de Administração e os relatórios sobre o funcionamento da aplicação serão enviados do dispositivo para o servidor de administração. Se as definições de funcionamento da aplicação não tiverem sido alteradas desde a última sincronização, as configurações da política não serão aplicadas.

2.1.10. Utilizar o Módulo Firewall

O módulo Firewall foi concebido para monitorizar a actividade de rede e a protecção do seu dispositivo móvel ao nível da rede (ver Figura 21).

Você pode seleccionar o nível de protecção (configuração **Firewall**) por forma a especificar o nível de controlo sobre o tráfego de entrada e saída, podendo escolher entre as opções sugeridas:

- **Elevado** – todas as actividades de rede estão bloqueadas, com excepção da actualização das bases e da ligação ao Kaspersky Administration Kit.
- **Médio** – todas as ligações de entrada estão bloqueadas. São permitidas as ligações de saída apenas a partir das portas SSH, HTTP, HTTPS, SMTP, IMAP.
- **Baixo** – apenas as ligações de entrada são bloqueadas.
- **Off** – todas as actividades de rede são permitidas.

Ao utilizar a configuração **Notificações**, você pode activar/desactivar a notificação do utilizador sobre uma tentativa de ligação com o nível de protecção seleccionado para a Firewall. Para desactivar a recepção de notificações, seleccione **Off**.

Figura 21. Separador **Firewall**

A informação sobre o funcionamento do módulo Firewall será registada nos relatórios da aplicação. Para visualizar o relatório, seleccione o item **Relatórios** no separador **Firewall**.

2.1.11. Visualizar relatórios sobre o funcionamento da aplicação

No separador **Informações**, pode visualizar o registo cronológico de eventos sobre o funcionamento do Kaspersky Mobile Security. Para o fazer, aceda a este separador e seleccione o item **Relatórios** (ver Figura 22).

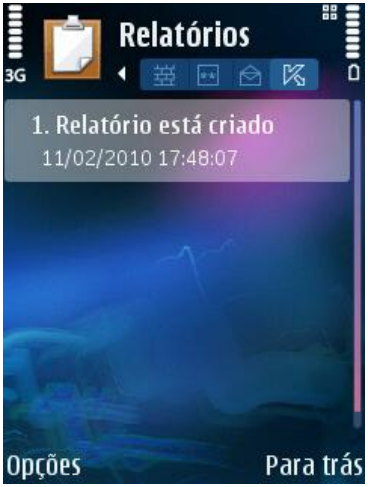

Figura 22. Relatório sobre o funcionamento da aplicação

2.2. Desinstalar a aplicação

Para desinstalar o Kaspersky Mobile Security, execute as seguintes acções:

1. Feche o Kaspersky Mobile Security. Para o fazer:
   a) Prima e mantenha premido o botão **Menu**.
   b) Seleccione o **KMS 7.0 EE** na lista de aplicações em execução e prima o botão **Opções**.
   c) Seleccione o item de menu **Sair** (ver Figura 23).

Figura 23. Fechar a aplicação

2. Desinstale o Kaspersky Mobile Security

   a) Prima o botão **Menu** e seleccione o item de menu **Gestor de Aplicações** (ver Figura 24).

Figura 24. Iniciar o **Gestor de Aplicações**

   b) Seleccione o **KMS7.0 EE** na lista de aplicações e prima o botão **Opções** (ver Figura 25).

Figura 25. Seleccionar a aplicação

c) Seleccione o item de menu **Remover** (ver Figura 26).

Figura 26. Desinstalar a aplicação

d) Para confirmar a remoção da aplicação, prima o botão **Sim** na janela de confirmação.

CAPÍTULO 3. KASPERSKY MOBILE SECURITY PARA MICROSOFT WINDOWS MOBILE

Este capítulo descreve o funcionamento do Kaspersky Mobile Security em dispositivos móveis com um dos seguintes sistemas operativos:

- Microsoft Windows Mobile 5.0.
- Microsoft Windows Mobile 6.0.

3.1. Começar

Esta secção contém informação sobre como iniciar a aplicação. Para além disso, também contém informação sobre os princípios gerais da interface gráfica do utilizador.

3.1.1. Iniciar a aplicação

Para iniciar o Kaspersky Mobile Security, execute as seguintes acções:

1. Abra o menu **Programas** no seu dispositivo móvel.
2. Seleccione o **KMS 7.0 EE** para iniciar a aplicação.

Depois de iniciar a aplicação, aparecerá uma janela com as principais componentes do Kaspersky Mobile Security (ver Figura 27) no ecrã do seu dispositivo móvel.

- **Prot. em Tempo Real** – utilização do modo de protecção em tempo real.
- **Última verificação** – data da última verificação anti-vírus do seu dispositivo móvel.
- **Última actualização –** data de distribuição da base de dados do Kaspersky Mobile Security utilizada pela aplicação.

> **Nota!**
>
> Se nunca tiver efectuado uma verificação anti-vírus do seu dispositivo móvel ou se tiverem passado duas semanas ou mais desde a última actualização da base de dados anti-vírus, o ícone junto ao item correspondente terá o seguinte aspecto: ⚠. Este ícone também aparecerá se o modo de protecção em tempo real ou se os módulos do Anti-Spam estiverem desactivados.

- **Firewall** – nível de protecção do dispositivo ao nível da rede.
- **Anti-Spam** – o estado do módulo Anti-Spam utilizado para filtrar as mensagens SMS.

> **Nota!**
>
> O módulo Anti-Spam não está disponível para PDA's!

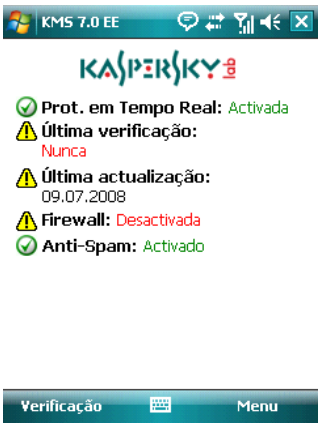

Figura 27. Janela de estado das componentes da aplicação

3.1.2. Interface Gráfica do Utilizador

A interface gráfica do utilizador consiste em seis separadores, aos quais pode aceder através do **Menu** (ver Figura 28):

- Ao utilizar o separador **Verificação**, pode executar uma verificação anti-vírus do dispositivo móvel, editar as configurações da verificação anti-vírus, da protecção em tempo real e da quarentena e criar o agendamento para a verificação automática (ver secção 3.2 na página 43).

- Ao utilizar a secção **Firewall**, pode monitorizar as actividades de rede e proteger o dispositivo ao nível da rede (ver secção 3.7 na página 59).
- Ao utilizar a secção **Actualização**, pode actualizar a base de dados anti-vírus, editar as configurações de actualização e configurar o agendamento para a actualização (ver secção 3.5 na página 57).
- Ao utilizar a secção **Anti-Spam**, pode configurar a filtragem de mensagens SMS recebidas (módulo Anti-Spam) (ver secção 3.4.1 na página 50).
- Ao utilizar a secção **Anti-Roubo**, pode bloquear o dispositivo e apagar informação guardada no mesmo em caso de roubo ou perda do seu dispositivo (módulo Anti-Roubo) (ver secção 3.4.2 na página 53).
- Ao utilizar o separador **Informações**, pode visualizar os registos sobre o funcionamento das componentes da aplicação, informação geral sobre a aplicação e as bases utilizadas (ver secção 3.8 na página 61).

Figura 28. Menu da aplicação

Para voltar à janela de estado das componentes da aplicação, seleccione o item **Ecrã de Estado**.

Para ver informação geral sobre a aplicação, seleccione o item **Sobre**.

Para fechar a aplicação, seleccione **Sair**.

3.2. Verificação anti-vírus e Protecção em Tempo Real

Através da secção **Verificação**, você pode executar uma verificação anti-vírus de todo o sistema de ficheiros e da memória do dispositivo ou de uma pasta ou ficheiro individual. Também pode alterar as configurações da verificação anti-vírus e da protecção anti-vírus em tempo real, visualizar o relatório sobre os resultados da verificação e criar o agendamento para o início automático da verificação.

3.2.1. Verificação sob pedido

Para alterar as configurações da verificação sob pedido:

1. Seleccione **Config. Verificação** na secção **Verificação**.
2. Defina a área de verificação na secção **Opções de Verificação**, seleccionando os tipos de ficheiros a verificar:
   - **Verificar arquivos** - verificar ficheiros compactados em arquivos.
   - **Apenas executáveis** - verificar apenas ficheiros de programas executáveis.
3. Na secção **Se um vírus for detectado**, determine a acção a executar pela aplicação quando for detectado um objecto infectado. Se a desinfecção não for necessária, seleccione a acção anti-vírus possível, escolhendo um dos seguintes valores para a configuração **Acção principal**:
   - **Quarentena** – move os objectos infectados para a quarentena.
   - **Perguntar ao Utilizador** - exibe uma mensagem no ecrã sobre a detecção de um vírus, com uma sugestão para apagar, colocar na quarentena ou ignorar o objecto infectado.
   - **Apagar** - apaga os objectos infectados detectados.
   - **Ignorar** – não executa qualquer acção com os objectos infectados.

   Se deseja que a aplicação tente desinfectar um objecto infectado detectado, assinale a caixa **Tentar desinfectar**. Na secção **Se a desinfecção falhar** seleccione uma acção a executar pela aplicação caso a desinfecção não seja possível.

Para iniciar uma verificação anti-vírus, execute as seguintes acções:

1. Inicie o Kaspersky Mobile Security (ver secção 3.1.1 na página 40).
2. Através da secção **Verificação** (ver Figura 29), seleccione o item **Verificar Telefone,** se desejar verificar todo o sistema de ficheiros do dispositivo móvel ou **Verificar Pasta**, se desejar verificar uma pasta individual.

Figura 29. Secção **Verificação**

Se tiver seleccionado o item **Verificar Pasta**, abrir-se-á uma janela que apresenta o sistema de ficheiros do dispositivo móvel. Para iniciar a verificação de uma pasta, mova o cursor para a pasta e clique no botão **Verificação**.

Depois de a verificação começar, abrir-se-á a janela de progresso da verificação, na qual será apresentado o actual estado da tarefa: o número de objectos verificados e o caminho para o objecto que está a ser verificado naquele momento (ver Figura 30).

Figura 30. Janela **Progresso da Verificação**

Figura 31. Notificação sobre a detecção de vírus

Depois de a verificação estar concluída, serão apresentadas as estatísticas gerais sobre os objectos maliciosos detectados e apagados.

3.2.2. Protecção em Tempo Real

A protecção em tempo real é o modo de funcionamento no qual a parte residente do Kaspersky Mobile Security permanece sempre na RAM (memória de acesso aleatório) do dispositivo móvel e verifica os ficheiros de programas executáveis e os ficheiros abertos pelo utilizador.

A protecção em tempo real é iniciada desde o momento em que o dispositivo é ligado e continua activa até este ser desligado (a não ser que este modo seja desactivado durante a configuração das definições de protecção).

O Kaspersky Mobile Security também permite efectuar uma verificação completa do sistema de ficheiros do dispositivo móvel.

Os resultados da protecção em tempo real e da verificação sob pedido serão registados no relatório. Para visualizar o relatório, seleccione o item **Relat. de Verificação**. Este relatório também está disponível na secção **Informações** (ver secção 3.8 na página 61).

Para activar o modo de protecção em tempo real:

1. Seleccione **Config. Protecção** na secção **Verificação**.
2. Assinale a caixa **Activ. Prot. Tempo Real**.

Para alterar as configurações de funcionamento da protecção em tempo real:

1. Seleccione **Configurações de protecção** na secção **Verificação**.
2. Assinale a caixa **Apenas executáveis** na secção **Opções de Verificação** se deseja que a protecção em tempo real apenas verifique os ficheiros de programas executáveis. Desmarque a caixa para fazer com que a protecção em tempo real verifique os ficheiros de programas executáveis e os ficheiros abertos pelo utilizador.
3. Na secção **Se um vírus for detectado**, seleccione a acção a executar pela aplicação quando for detectado um objecto infectado. Pode seleccionar uma das seguintes opções:
    - **Quarentena** – move os objectos infectados detectados para a quarentena.
    - **Apagar** - apaga os objectos infectados detectados.
    - **Ignorar** – não executa qualquer acção com os objectos infectados.

3.2.3. Verificação agendada

O Kaspersky Mobile Security permite ao utilizador criar o agendamento para a verificação automática do dispositivo móvel. A verificação é executada em segundo plano. Ao detectar um objecto infectado, a acção especificada nas configurações de verificação será executada com esse objecto (o item **Config. Verificação**).

Por defeito, a verificação agendada está desactivada.

Para criar um agendamento para a inicialização da verificação do sistema de ficheiros de um dispositivo:

Na secção **Verificação**, seleccione o item **Agendamento** e crie um agendamento para a inicialização de verificação (ver Figura 32):

- **Diariamente** - a verificação será efectuada todos os dias. A hora da verificação é determinada pela configuração **Hora**.
- **Semanalmente** - a verificação será efectuada uma vez por semana. A data e hora da verificação será determinada pelas configurações **Dia da semana** e **Hora**.
- **Manual** - a verificação será manualmente iniciada pelo utilizador.

Figura 32. Menu **Agendamento**

3.3. Utilizar a Quarentena

Os objectos infectados colocados na quarentena não representam qualquer ameaça para o seu dispositivo móvel e podem ser apagados ou restaurados mais tarde.

A aplicação pode colocar os objectos infectados na quarentena, automaticamente ou após a sua confirmação.

Para activar a colocação automática dos objectos infectados na quarentena:

1. Abra a secção **Verificação**.
2. Seleccione o item **Config. Verificação**.
3. Na secção **Se um vírus for detectado**, seleccione **Quarentena** como a acção a executar pela aplicação no caso de detecção de um objecto de software malicioso.

   Se seleccionou **Perguntar ao Utilizador** como a acção a executar, então quando for detectado um objecto infectado, aparecerá uma janela de notificação a perguntar se deseja apagar o objecto ou colocá-lo na quarentena.

Para ver o conteúdo da quarentena,

abra a secção **Verificação** e seleccione o item **Quarentena** (ver Figura 33).

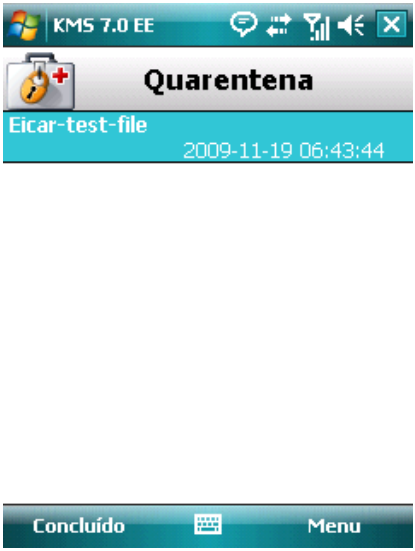

Figura 33. **Quarentena**

O **Menu**, acessível a partir da janela de visualização da quarentena, permite ao utilizador:

- Ver informação detalhada sobre o objecto seleccionado na quarentena (item **Informação detalhada**).
- Apagar o objecto seleccionado (item **Apagar Ficheiro**).
- Restaurar o objecto actual da Quarentena para a sua pasta original (item **Restaurar**).
- Limpar a quarentena, apagando todos os objectos em quarentena (item **Esvaziar quarentena**).

3.4. Utilizar os módulos Anti-Spam e Anti-Roubo

O módulo Anti-Spam foi concebido para assegurar a protecção do seu dispositivo contra mensagens SMS indesejadas.

A filtragem baseia-se na utilização das listas "negra" e "branca". Estas listas contém números de telefone e exemplos de frases características de

mensagens spam e não-spam. A análise de mensagens será efectuada pela seguinte ordem:

- verificar se o número do remetente está incluído na lista "negra";
- verificar se o número do remetente está incluído na lista "branca";
- verificação do texto da mensagem quanto à presença de frases existentes na lista “negra”;
- verificação do texto da mensagem quanto à presença de frases existentes na lista “branca”;

Se for detectada pelo menos uma correspondência, a verificação será interrompida. A mensagem que contenha um elemento existente na lista “negra” será bloqueada. A mensagem que contenha um elemento existente na lista “branca” será permitida.

3.4.1. Módulo Anti-Spam

O módulo Anti-Spam foi concebido para assegurar a protecção do seu telemóvel contra mensagens SMS indesejadas.

Nota!

O módulo Anti-Spam não está disponível para PDA’s!

A filtragem baseia-se na utilização das listas "negra" e "branca". Estas listas contém números de telefone e exemplos de frases características de mensagens spam e não-spam. A análise de mensagens será efectuada pela seguinte ordem:

- verificar se o número do remetente está incluído na lista "negra";
- verificar se o número do remetente está incluído na lista "branca";
- verificação do texto da mensagem quanto à presença de frases existentes na lista “negra”;
- verificação do texto da mensagem quanto à presença de frases existentes na lista “branca”;

Se for detectada pelo menos uma correspondência, a verificação será interrompida. A mensagem que contenha um elemento existente na lista “negra” será bloqueada. A mensagem que contenha um elemento existente na lista “branca” será permitida.

Para alterar as configurações do Anti-Spam:

1. Seleccione **Configurações** na secção **Anti-Spam**.

2. Seleccione o modo de funcionamento através da configuração **Anti-Spam**:

   - **Normal.** Neste modo, o Anti-Spam filtra as mensagens recebidas através das listas "negra" e "branca". Quando for recebida uma mensagem de um número de telefone não incluído em nenhuma das listas, o Anti-Spam notificará o utilizador e dar-lhe-á a opção de bloquear ou permitir a recepção da mensagem e ainda a opção de adicionar este número de telefone à lista "branca" ou "negra".
   - **Apenas Lista Negra.** Neste modo, o Anti-Spam bloqueia a recepção das mensagens que correspondam aos critérios da "lista negra". Todas as outras mensagens serão permitidas.
   - **Apenas Lista Branca.** Neste modo, o Anti-Spam permite as mensagens que correspondam aos critérios da "lista branca". Todas as outras mensagens serão bloqueadas.
   - **Desactivado.** Neste modo, o Anti-Spam está desactivado. Não é efectuada a filtragem das mensagens recebidas.

3. Assinale a caixa **Adicionar à Lista Branca** de forma a que o Anti-Spam não bloqueie a recepção de mensagens de números incluídos na lista de contactos.
4. Assinale a caixa **Bloquear Não Num.** de forma a que o Anti-Spam bloqueie a recepção de mensagens de números não numéricos.

3.4.1.1. Editar as listas "negra" e "branca"

A lista "Negra" contém registos que, quando detectados em mensagens, fazem com que o Anti-Spam bloqueie essas mensagens.

A lista "Branca" contém registos que, quando detectados em mensagens, fazem com que o Anti-Spam permita essas mensagens.

Para editar a lista "negra" ou a lista "branca",

abra a secção **Anti-Spam** (ver Figura 34) e seleccione a lista correspondente.

Para editar a lista, utilize o **Menu**:

- **Inserir número** – adicionar um novo registo à lista.
- **Apagar número** – apagar o registo da lista.
- **Editar número** – editar o registo actual da lista.

Seleccione o item **Inserir número** e especifique o número de telefone (campo **Inserir telefone**) que deseja incluir na lista. Este número pode começar com um

dígito ou um "+". Para além disso, ao especificar um número, pode utilizar as máscaras "?" e "*".

Também pode especificar o texto (campo **Inserir texto**), cuja detecção numa mensagem recebida fará com que sejam executadas as seguintes acções:

- a mensagem na qual é detectado o texto especificado na lista “branca” será permitida;
- a mensagem na qual é detectado o texto especificado na lista "negra" será bloqueada;

Figura 34. Secção **Anti-Spam**

Depois de terminar de editar a lista, prima **Concluído** para voltar à secção **Anti-Spam**.

3.4.1.2. Acções a executar em relação às mensagens

Quando receber mensagens de um número de telefone não incluído nas listas "negra" ou "branca", dependendo se as configurações do Anti-Spam permitem a recepção de mensagens de números desconhecidos (ver secção 3.4.1 na página 50), será exibido um aviso no ecrã do dispositivo móvel (ver Figura 35).

Figura 35. Aviso do Anti-Spam

Através do **Menu**, pode seleccionar uma das seguintes acções a serem executadas com a mensagem:

- **Adicionar à Lista Branca** – permite a recepção da mensagem e adiciona o número de telefone do remetente à lista "branca".
- **Adicionar à Lista Negra** – bloqueia a recepção da mensagem e adiciona o número de telefone do remetente à lista "negra".

Prima o botão **Ignorar**, para permitir a recepção da mensagem. Neste caso, o número de telefone do remetente não será adicionado a nenhuma das listas.

A informação sobre as mensagens bloqueadas será registada nos relatórios da aplicação.

Para visualizar o relatório, seleccione o botão **Relat. do Anti-Spam** na secção **Anti-Spam.** O relatório também está disponível na secção **Informações** (ver secção 3.8 na página 60);

3.4.2. Separador Anti-Roubo

Este módulo Anti-Roubo (secção **Anti-Roubo**) (ver Figura 36) foi concebido para garantir a protecção dos dados armazenados no dispositivo móvel contra o acesso não-autorizado, no caso de o dispositivo ser roubado ou perdido.

Quando aceder às configurações do módulo pela primeira vez, terá de definir uma password. Ao utilizar esta password, você pode aceder às configurações do módulo para activar as funções do módulo. A password é necessária para impedir o acesso não-autorizado às configurações de funcionamento do módulo e para permitir ao utilizador bloquear e apagar informações guardadas no dispositivo em caso de roubo ou perda.

Função **Bloqueio por SMS** – permite bloquear o dispositivo por ordem do utilizador. Você pode desbloquear o dispositivo apenas depois de inserir uma password utilizada para aceder ao módulo Anti-Roubo. A acção desta função é accionada depois de o utilizador enviar uma mensagem SMS: "`block:code`" para o dispositivo perdido.

A **Limpeza por SMS** permite apagar a informação pessoal do utilizador (contactos, mensagens recebidas, ficheiros pessoais, configurações da ligação de rede). A acção desta função é accionada depois de o utilizador enviar uma mensagem SMS: "`clean:code`" para o dispositivo perdido.

A **Protecção Cartão SIM** permite enviar para os números especificados um novo número de telefone, em caso de perda do dispositivo, e assim bloquear este dispositivo. Você pode desbloquear o dispositivo inserindo a password definida para aceder ao módulo Anti-Roubo.

Se for necessário alterar a password utilizada para trabalhar com o módulo Anti-Roubo, seleccione o item **Alterar código**. Insira a nova password e a respectiva confirmação e prima o botão **Concluído**.

Figura 36. Secção **Anti-Roubo**

A informação sobre o funcionamento do módulo Anti-Roubo será registada nos relatórios da aplicação. Para visualizar o relatório, seleccione o item **Relatório** na secção **Anti-Roubo**. O relatório também está disponível na secção **Informações** (ver secção 3.8 na página 61).

3.4.2.1. Configurações da função Limpeza por SMS

A função **Limpeza por SMS** permite apagar dados do dispositivo em caso de perda (ver Figura 37).

Para alterar as configurações da função Limpeza por SMS:

1. Abra a secção **Anti-Roubo**.
2. Insira a password e seleccione **Limpeza por SMS** na janela que se abre.
3. Assinale a caixa **contactos**, se deseja que a lista de contactos seja apagada caso o seu dispositivo móvel seja roubado ou perdido.
4. Assinale a opção **caixa de entrada**, se deseja apagar e-mails, mensagens SMS.
5. Assinale a caixa **documentos**, se deseja apagar os ficheiros pessoais do utilizador.
6. Assinale a caixa **configurações de rede**, se deseja apagar as configurações da ligação de rede.
7. Assinale a caixa **ficheiros no cartão** se deseja apagar os ficheiros do cartão de memória do dispositivo.
8. Prima **Concluído** para guardar as alterações.

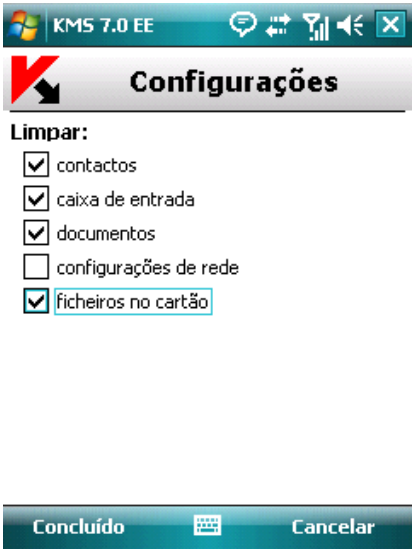

Figura 37. Configurações da Limpeza por SMS

3.4.2.2. Configurações da função Protecção do Cartão SIM

A função **Protecção do Cartão SIM** foi concebida para monitorizar a substituição do cartão SIM no dispositivo (ver Figura 38).

Para alterar as configurações da função Protecção do Cartão SIM:

1. Abra a secção **Anti-Roubo**.
2. Insira a password e seleccione a **Protecção do Cartão SIM** na janela que se abre.
3. Nos campos **1)** e **2)** insira os números de telefone para os quais gostaria de receber um novo número de telefone se o cartão SIM for substituído no seu dispositivo. Estes números podem começar com um dígito ou um "+" e têm de conter unicamente dígitos.
4. Assinale a caixa **Bloquear** para activar o bloqueio do dispositivo caso o cartão SIM seja substituído.
5. Prima **Concluído** para guardar as alterações que efectuou.

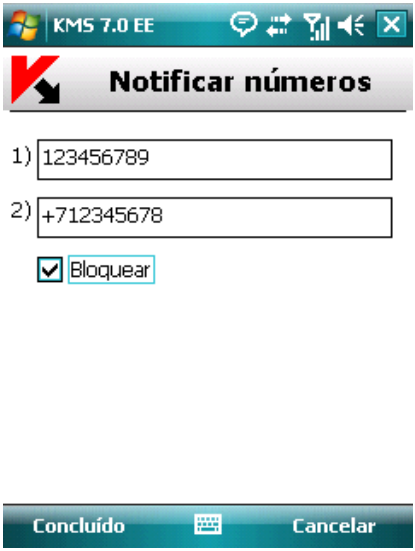

Figura 38. Configurações da **Protecção do Cartão SIM**

3.5. Actualizar as bases da aplicação

A verificação de programas maliciosos é executada com base nos registos das bases do Kaspersky Mobile Security, que contêm a descrição de todos os programas maliciosos actualmente conhecidos. Por essa razão, é extremamente importante manter as suas bases actualizadas.

Você pode actualizar as bases manualmente ou de acordo com um agendamento. Para configurar e iniciar a actualização, utilize o separador **Actualização** (ver Figura 39). As actualizações são efectuadas a partir dos servidores de actualização da Kaspersky Lab, através da Internet.

A informação sobre a actualização das bases será registada nos relatórios da aplicação. Para visualizar o relatório, seleccione o item **Relat. de Actualização** na secção **Actualização**. O relatório também está disponível na secção **Informações** (ver secção 3.8 na página 61).

Figura 39. Secção **Actualização**

Para iniciar, manualmente, a actualização das bases da aplicação, execute as seguintes acções:

1. Inicie o Kaspersky Mobile Security (ver secção 3.1.1 na página 40) e abra a secção **Actualização**.
2. Seleccione **Actualização** para iniciar a transferência das actualizações.

Para criar um agendamento para a inicialização da actualização das bases da aplicação:

1. Inicie o Kaspersky Mobile Security (ver secção 3.1.1 na página 40) e abra a secção **Actualização**.
2. Seleccione o item **Agendamento**.
3. Especifique a frequência das actualizações na secção **Actualização Autom.**:
   - **Diariamente** - a actualização será efectuada todos os dias. Para além disso, especifique a **Hora** da actualização.
   - **Semanalmente** - a actualização será efectuada uma vez por semana. Para além disso, especifique o **Dia da semana** e a **Hora** da actualização.
   - **Manual** – a actualização será manualmente iniciada pelo utilizador.

Na secção **Informações**, pode verificar a data de distribuição das bases da aplicação, assim como o número de assinaturas de vírus. Para o fazer, seleccione o item **Sobre as bases** neste separador.

3.6. Actualizar as configurações de funcionamento da aplicação

Nota

Para mais detalhes sobre o funcionamento conjunto do Kaspersky Mobile Security e do Kaspersky Administration Kit, consulte o Manual de Administrador do Kaspersky Mobile Security.

Ao utilizar o Kaspersky Mobile Security juntamente com o Kaspersky Administration Kit, as configurações de funcionamento da aplicação serão definidas pela política para um grupo de dispositivos móveis. A activação da aplicação e a implementação das configurações da política bloqueadas para impedir alterações irão ocorrer quando um dispositivo for adicionado ao grupo de administração.

Mais tarde, a sincronização da aplicação com o Servidor de Administração será, automaticamente, executada em intervalos definidos nas configurações da política.

Para iniciar a sincronização manual da aplicação com o Servidor de Administração:

1. Inicie o Kaspersky Mobile Security (ver secção 2.1.1 na página 9).
2. Abra a secção **Actualização**.
3. Seleccione o item **Sincronizar**.

Durante a sincronização, as configurações de funcionamento da aplicação serão carregadas a partir do Servidor de Administração e os relatórios sobre o funcionamento da aplicação serão enviados do dispositivo para o servidor de administração. Se as definições de funcionamento da aplicação não tiverem sido alteradas desde a última sincronização, as configurações da política não serão aplicadas.

3.7. Firewall

O módulo **Firewall** foi concebido para monitorizar a actividade de rede e a protecção do seu dispositivo móvel ao nível da rede (ver Figura 40).

Para alterar as configurações de funcionamento da Firewall:

1. Inicie o Kaspersky Mobile Security (ver secção 3.1.1 na página 40) e abra a secção **Firewall**.
2. Seleccione o item **Configurações da Firewall**. Na janela que se abre, defina o nível de protecção para especificar o nível de monitorização do tráfego de entrada e saída. Pode escolher entre as seguintes opções:
   - **Bloquear toda** – todas as actividades de rede estão bloqueadas, com excepção da actualização das bases e da ligação ao Kaspersky Administration Kit.
   - **Médio** – todas as ligações de entrada serão bloqueadas. São permitidas as ligações de saída apenas a partir das portas SSH, HTTP, HTTPS, SMTP, IMAP.
   - **Baixo** – apenas as ligações de entrada são bloqueadas.
   - **Desactivada** – todas as actividades de rede são permitidas.

A informação sobre o funcionamento da Firewall será registada nos relatórios da aplicação. Para visualizar o relatório, seleccione o item **Relatório da Firewall** na secção **Firewall**.

Figura 40. Secção **Firewall**

3.8. Visualizar relatórios sobre o funcionamento da aplicação

Os relatórios sobre o funcionamento da aplicação estão presentes no item **Relatórios** do separador **Informações**. Pode ver um relatório sobre qualquer tarefa executada pelo Kaspersky Mobile Security:

- verificação anti-vírus;
- actualização das bases da aplicação;
- funcionamento da firewall;
- funcionamento do módulo Anti-Spam;
- funcionamento do módulo Anti-Roubo.

Para visualizar o relatório sobre o funcionamento de uma das componentes da aplicação:

1. Inicie o Kaspersky Mobile Security (ver secção 3.1.1 na página 40).
2. Seleccione o item **Relatórios** no separador **Informações** (ver Figura 41).
3. Na janela que se abre, seleccione o relatório da componente desejada.

Figura 41. Secção **Relatórios**

3.9. Desinstalar a aplicação

Para desinstalar o Kaspersky Mobile Security, execute as seguintes acções:

1. Desactive a Protecção em Tempo Real (para mais detalhes, veja a secção 3.2 na página 43);

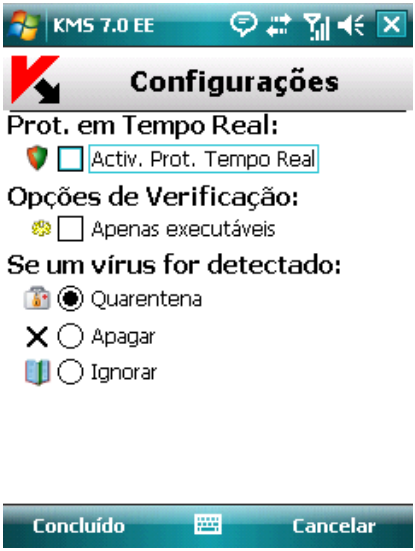

Figura 42. Desactivar a protecção em tempo real

2. Feche o Kaspersky Mobile Security. Para o fazer, seleccione o item de menu **Sair** (ver Figura 43).

Figura 43. Fechar a aplicação

3. Desinstale a aplicação. Para o fazer:

   a) prima o botão **Iniciar**, seleccione o menu **Configurações**, abra o separador **Sistema** e depois seleccione **Remover programas** (ver Figura 44):

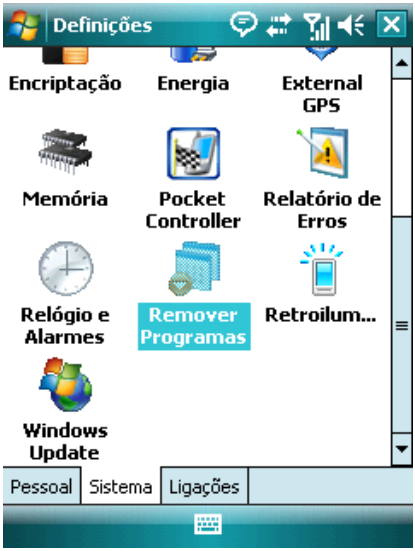

Figura 44. Iniciar a remoção da aplicação

   b) Seleccione o **Kaspersky Mobile Security** na lista de aplicações instaladas e prima o botão **Remover** (ver Figura 45).

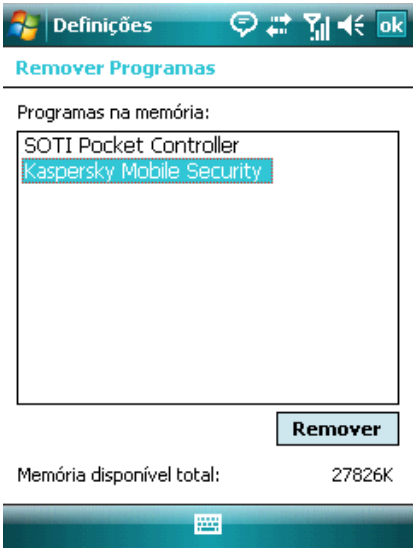

Figura 45. Seleccionar a aplicação

c) Prima o botão **Sim** na janela de confirmação da remoção da aplicação (ver Figura 46). Depois disso, abrir-se-á uma notificação sobre a remoção do ficheiro que contém as configurações de funcionamento da aplicação. Prima **Não** para desinstalar a aplicação por completo. Se premir o botão **Sim**, o ficheiro com as configurações de funcionamento da aplicação será mantido no dispositivo.

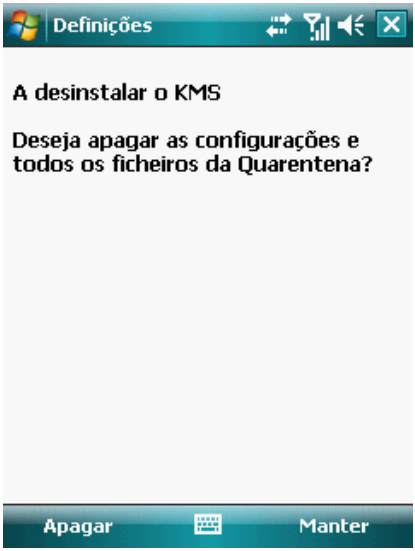

Figura 46. Aviso para guardar as configurações de funcionamento da aplicação

APÊNDICE A. KASPERSKY LAB

A Kaspersky Lab foi fundada em 1997 e actualmente é a empresa russa líder no desenvolvimento de uma vasta gama de produtos de software de segurança de informação, incluindo sistemas antivírus, anti-spam e anti-hackers.

A Kaspersky Lab é uma empresa internacional. Sediada na Federação Russa, a empresa tem filiais representantes no Reino Unido, França, Alemanha, Japão, Benelux, China, Polónia, Roménia e EUA (Califórnia). Um novo departamento da empresa, o Centro Europeu de Pesquisa Antivírus, foi recentemente criado em França. A rede de parceiros da Kaspersky Lab inclui mais de 500 empresas em todo o mundo.

Hoje, a Kaspersky Lab emprega mais de 1000 especialistas altamente qualificados, dos quais 10 têm graduações M.B.A. e 16 têm doutoramentos. Vários especialistas antivírus seniores da Kaspersky Lab são membros da Computer Anti-virus Researchers Organization (CARO).

Os bens mais valiosos da nossa empresa são a experiência e o conhecimento únicos acumulados pelos nossos especialistas ao longo de 14 anos a combater vírus de computador. Uma análise detalhada das actividades dos vírus de computador permite que os especialistas da empresa consigam prever as tendências no desenvolvimento de software malicioso e forneçam aos nossos utilizadores uma protecção atempada contra novos tipos de ataques. Esta vantagem é a base dos produtos e serviços da Kaspersky Lab. Em qualquer altura, os produtos da empresa permanecem um passo à frente dos outros fornecedores no fornecimento de uma cobertura antivírus abrangente para os nossos clientes.

Anos de árduo trabalho tornaram a empresa num dos melhores fabricantes de software antivírus. A Kaspersky Lab foi a primeira empresa a desenvolver muitos dos padrões modernos de software antivírus. O produto emblemático da empresa, o Kaspersky Anti-Virus®, protege com fiabilidade todos os tipos de sistemas de computadores contra ataques de vírus, incluindo estações de trabalho, servidores de ficheiros, sistemas de correio electrónico, firewalls, gateways de Internet e computadores portáteis. As suas ferramentas de gestão fáceis de utilizar maximizam o nível de automação da protecção antivírus para computadores e redes empresariais. Um grande número fabricantes a nível mundial usa o núcleo do Kaspersky Anti-Virus nos seus produtos, incluindo a Nokia ICG (EUA), Aladdin (Israel), Sybari (EUA), G Data (Alemanha), Deerfield (EUA), Alt-N (EUA), Microworld (Índia) e BorderWare (Canadá).

Os clientes da Kaspersky Lab beneficiam de uma ampla gama de serviços adicionais que asseguram tanto o funcionamento estável dos produtos da empresa, como a total conformidade com as necessidades específicas dos clientes. Concebemos, implementamos e damos apoio a sistemas empresariais antivírus. A base de dados antivírus da Kaspersky Lab é actualizada a cada

hora. A empresa fornece aos seus clientes um serviço de suporte técnico de 24 horas, disponível em várias línguas.

Se tiver alguma questão, comentário ou sugestão, pode contactar-nos através dos nossos distribuidores ou contactar, directamente, a Kaspersky Lab. Teremos todo o prazer em ajudá-lo por telefone ou por e-mail em qualquer assunto relacionado com nossos produtos. Receberá respostas completas e abrangentes a todas as suas questões.

Site oficial da Kaspersky Lab:	http://www.kaspersky.pt
Enciclopédia de Vírus:	http://www.viruslist.com
Laboratório Antivírus:	newvirus@kaspersky.com (apenas para enviar objectos suspeitos em arquivos) http://support.kaspersky.ru/virlab/helpdesk.html?LANG=en (para enviar pedidos aos analistas de vírus)
Fórum na Internet da Kaspersky Lab:	http://forum.kaspersky.com

APÊNDICE B. CRYPTOEX LLC

Para criar e verificar as assinaturas digitais, o Kaspersky Internet Security utiliza a biblioteca de software de segurança de dados Crypto C desenvolvida pela Crypto Ex LLC. A Crypto Ex detém uma licença da Agência Federal de Informações e Comunicações Governamentais (FSB - Serviço Federal de Segurança) e o certificado da biblioteca de software de segurança de dados Crypto C.

Site empresarial da CryptoEx LLC: http://www.cryptoex.ru

Os direitos exclusivos da biblioteca de software de segurança de dados pertencem à CryptoEx LLC.

APÊNDICE C. CONTRATO DE LICENCA DE UTILIZADOR FINAL DO KASPERSKY LAB

Contrato Padrão de Licença de Utilizador Final

AVISO LEGAL IMPORTANTE A TODOS OS UTILIZADORES: LEIA COM ATENÇÃO O SEGUINTE ACORDO LEGAL ANTES DE COMEÇAR A UTILIZAR O SOFTWARE.

AO CLICAR NO BOTÃO "ACEITAR" NA JANELA DO CONTRATO DE LICENÇA OU AO INTRODUZIR SÍMBOLO(S) CORRESPONDENTE(S) CONCORDA EM ESTAR VINCULADO PELOS TERMOS E CONDIÇÕES DESTE CONTRATO. **ESSA ACÇÃO SIMBOLIZA A SUA ASSINATURA E ESTÁ A CONCORDAR ESTAR VINCULADO AO CONTRATO, CONSTITUINDO UMA PARTE DO MESMO, E CONCORDA QUE ESTE CONTRATO É EXECUTÓRIO COMO QUALQUER OUTRO CONTRATO NEGOCIADO POR ESCRITO E ASSINADO POR SI.** SE NÃO CONCORDAR COM TODOS OS TERMOS E CONDIÇÕES DESTE CONTRATO, CANCELE A INSTALAÇÃO DO SOFTWARE E NÃO O INSTALE.

O SOFTWARE PODE SER ACOMPANHADO POR UM CONTRATO ADICIONAL OU OUTRO DOCUMENTO SEMELHANTE ("CONTRATO ADICIONAL") QUE PODE DEFINIR O NÚMERO DE COMPUTADORES ONDE SE PODE USAR O SOFTWARE, O PERÍODO DE UTILIZAÇÃO DO SOFTWARE, TIPO DE OBJECTOS PRETENDIDOS COM O USO DO SOFTWARE E OUTRAS CONDIÇÕES DA COMPRA, AQUISIÇÃO E USO. ESTE CONTRATO ADICIONAL CONSTITUI PARTE ***INTEGRANTE DO CONTRATO DE LICENÇA.***

DEPOIS DE CLICAR NO BOTÃO "ACEITAR" NA JANELA DO CONTRATO DE LICENÇA OU APÓS TER INTRODUZIDO O(S) SÍMBOLO(S) CORRESPONDENTE(S), TEM O DIREITO DE UTILIZAR O SOFTWARE DE ACORDO COM OS TERMOS E CONDIÇÕES DESTE CONTRATO.

1. Definições

1.1. **Software** refere-se ao software, incluindo quaisquer Actualizações e materiais relacionados.

1.2. **Detentor dos Direitos** (proprietário de todos os direitos, quer exclusivos ou relativos ao Software) refere-se à Kaspersky Lab ZAO, uma empresa incorporada de acordo com as leis da Federação Russa.

1.3. **Computador(es)** refere-se ao(s) hardware(s), incluindo os computadores pessoais, portáteis, estações de trabalho, assistentes digitais pessoais, 'smart phones', dispositivos manuais ou outros dispositivos electrónicos para os quais o Software foi concebido e onde o Software será instalado e/ou usado.

1.4. **Utilizador Final** refere-se ao(s) indivíduo(s) que instalam ou utilizam o Software a seu favor ou que utilizam legalmente uma cópia do Software; ou, se o Software for transferido ou instalado em nome de uma organização, quando se refere a um funcionário, *"Utilizador Final"* refere-se ainda à organização para a qual o Software foi transferido ou instalado ficando por este meio claramente definido que essa organização autorizou a pessoa que aceitou este contrato a fazê-lo em seu nome. Para fins deste contrato, o termo *"organização",* sem limitações, inclui quaisquer parcerias, empresas de responsabilidade limitada, corporações, associações, empresas de capitais mistos, empresas de crédito, "joint ventures", sindicatos de trabalho, empresas não constituídas em sociedade ou autoridades governamentais.

1.5. **Parceiro(s)** refere-se a organizações ou indivíduo(s), que distribuem o Software com base num contrato e numa licença do Detentor dos Direitos.

1.6. **Actualização(ões)** refere-se a todas as actualizações, revisões, correcções ("patches"), melhorias, "fixes", modificações, cópias, adições ou pacotes de manutenção, etc.

1.7. **Manual do Utilizador** refere-se ao manual do utilizador, guia do administrador, livro de referências e material explicativo ou de outro tipo relacionado.

1.8. **Aquisição do Software** refere-se à compra do Software ou à aquisição do Software nos termos definidos em contratos adicionais, incluindo a aquisição a título gratuito.

2. Concessão de licença

2.1. O Detentor de Direitos concede, por este meio, uma licença de não exclusividade ao Utilizador Final que lhe permite armazenar, carregar, instalar, executar e visualizar (para "utilizar") o Software num número específico de Computadores, tendo como finalidade ajudar a proteger o Computador do Utilizador Final no qual o Software está instalado, contra as ameaças descritas no Manual do Utilizador, de acordo com todos os requisitos técnicos descritos no Manual do Utilizador e com os termos e condições deste Contrato (a "Licença") e o utilizador final aceita esta Licença:

Versão experimental. Se recebeu, transferiu e/ou instalou uma versão experimental do Software sendo-lhe por este meio concedida uma

licença de avaliação para o Software, só pode utilizar o Software para fins de avaliação e apenas durante o período de avaliação único aplicável, a não ser se indicado o contrário, a contar da data da instalação inicial. A utilização do Software para outros fins ou para além do período de avaliação aplicável é estritamente proibida.

Software de vários ambientes; Software de vários idiomas; Software de dualidade de multimédia; várias cópias; pacotes. Se utilizar versões diferentes do Software ou edições do Software em idiomas diferentes, se receber o Software em vários suportes, se receber várias cópias do Software ou se receber o Software num pacote junto com outro software, o número total permitido de Computadores em que as versões do Software estão instaladas devem corresponder ao número total de computadores especificados nas licenças obtidas junto do Detentor dos Direitos e, *a não ser* que os termos da licença indiquem o contrário, cada licença adquirida dá-lhe o direito de instalar e utilizar o Software nessa quantidade de Computador(es), como especificado nas Cláusulas 2.2 e 2.3.

2.2. Se o Software foi adquirido num meio físico, o Utilizador Final tem o direito de utilizar o Software para protecção na quantidade de Computador(es) especificada na embalagem do Software ou especificada no contrato adicional.

2.3. Se o Software foi adquirido através da Internet, o Utilizador Final tem o direito de utilizar o Software para protecção na quantidade de Computador(es) especificada na Licença do Software ou no contrato adicional quando este foi adquirido.

2.4. Tem o direito de fazer uma cópia do Software apenas para fins de cópia de segurança e apenas para substituir a cópia legal caso essa cópia se perca, seja destruída ou fique inutilizada. Esta cópia de segurança não pode ser utilizada para outros fins e tem de ser destruída se perder o direito de utilização do Software ou quando a licença de Utilizador Final expirar ou for rescindida por qualquer outra razão, de acordo com a legislação em vigor no país de residência principal do Utilizador Final ou no país onde o mesmo está a utilizar o Software.

2.5. A partir do momento em que o Software foi activado ou que o ficheiro da chave de licença foi instalado (à excepção de uma versão experimental do Software), tem o direito de receber os seguintes serviços pelo período definido especificado na embalagem de Software (se o Software foi adquirido num meio físico) ou especificado durante a aquisição (se o Software foi adquirido através da Internet):

- Actualizações do Software através da Internet quando e como o Detentor dos Direitos os publicar no seu próprio website ou através de outros serviços online. Quaisquer Actualizações que possa receber passam a fazer parte do Software e os termos e condições deste Contrato aplicam-se às mesmas;

- Assistência técnica através da Internet e assistência técnica através de uma linha telefónica grátis.

3. Activação e Termo

3.1. Se o Utilizador Final modificar o seu Computador ou fizer alterações ao software de outros fabricantes instalado nesse mesmo Computador, o Detentor dos Direitos poderá exigir que repita a activação do Software ou a instalação do ficheiro da chave de licença. O Detentor dos Direitos reserva-se o direito de utilizar quaisquer meios ou procedimentos de verificação para confirmar a validade da Licença e/ou a legalidade de uma cópia instalada do Software e/ou utilizada no Computador do Utilizador Final.

3.2. Se o Software foi adquirido num meio físico, o Software pode ser utilizado, mediante a sua aceitação deste Contrato, pelo período especificado na embalagem. Esse período terá início a partir do momento de aceitação deste Contrato ou nos termos especificados no contrato adicional.

3.3. Se o Software foi adquirido através da Internet, o Software pode ser utilizado, mediante a sua aceitação deste Contrato, pelo período especificado durante a aquisição ou nos termos especificados no contrato adicional.

3.4. Tem o direito de utilizar uma versão experimental do Software, como disposto na Cláusula 2.1 sem que tenha de pagar nada durante o período de avaliação (30 dias) desde o momento em que o Software é activado, de acordo com este Contrato, *desde que* a versão experimental não de ao Utilizador Final acesso a Actualizações e a assistência técnica através da Internet e da linha telefónica.

3.5. A Licença para Utilização do Software está limitada ao período de tempo especificado nas Cláusulas 3.2 ou 3.3 (como aplicável) e o restante período pode ser visto através dos meios descritos no Manual do Utilizador.

3.6. Se tiver adquirido o Software que se destina a ser usado em mais do que um Computador, a sua Licença para Usar o Software estará limitada ao período de tempo que tem início com a data de activação do Software ou da instalação do ficheiro da chave de licença no primeiro Computador.

3.7. Sem prejuízo de quaisquer recursos legais ou de justiça natural que o Detentor dos Direitos possa ter, caso haja alguma violação de qualquer parte dos termos e condições deste Contrato por parte do Utilizador Final, o Detentor dos Direitos pode, em qualquer altura e sem qualquer aviso prévio ao Utilizador Final, rescindir esta Licença de utilização do Software sem reembolsar o preço de compra ou qualquer outra parte do mesmo.

3.8. Concorda que, ao utilizar o Software e qualquer relatório ou informações derivadas resultantes da utilização deste Software, irá

cumprir todas as leis e regulamentos internacionais, nacionais, estatais, regionais e locais aplicáveis, incluindo, mas não se limitando às leis da privacidade, direitos de autor, controlo de exportação e obscenidade.

3.9. Excepto quando especificamente indicado neste documento, não pode transferir nem atribuir a terceiros nenhum dos direitos a si concedidos, ao abrigo deste Contrato, nem nenhuma das suas obrigações em conformidade com o presente.

4. Assistência técnica

A assistência técnica descrita na Cláusula 2.5 deste Contrato é fornecida ao Utilizador Final depois de ter sido instalada a mais recente Actualização do Software (excepto quando se trata de uma versão experimental do Software).
Serviço de assistência técnica: http://support.kaspersky.com

5. Limitações

5.1. Não deve emular, clonar, alugar, emprestar, arrendar, vender, modificar, descompilar ou inverter a engenharia do Software, nem desmontar ou criar trabalhos dele derivados e baseados no Software ou em qualquer parte do mesmo, sendo que a única excepção é a existência de um direito sem limitações concedido ao Utilizador Final pela legislação aplicável, bem como não pode reduzir qualquer parte do Software a uma forma legível, nem transferir o Software licenciado, ou qualquer outro subconjunto do Software licenciado, nem permitir que terceiros o façam, excepto até ao ponto em que as restrições indicadas sejam expressamente proibidas pela lei aplicável. Não se pode utilizar o código de binários nem a fonte do Software, nem inverter a engenharia, para recriar o algoritmo do programa, que é registado. Todos os direitos que não são aqui expressamente concedidos são reservados pelo Detentor dos Direitos e/ou pelos seus fornecedores, como aplicável. Qualquer utilização não autorizada do Software resultará na rescisão imediata e automática deste Contrato e da Licença concedida pelo mesmo e pode resultar em processos criminais e/ou civis contra o Utilizador Final.

5.2. Não pode transferir os direitos de utilização do Software para terceiros, excepto conforme disposto no contrato adicional.

5.3. Não pode fornecer o código de activação e/ou a ficheiro com a chave da licença a terceiros nem permitir que terceiros acedam ao código de activação e/ou chave da licença que são considerados dados confidenciais do Detentor dos Direitos e terá todo o cuidado em proteger o código de activação e/ou chave da licença contando que pode transferir o código de activação e/ou a chave de licença a terceiros como definido no contrato adicional.

5.4. Não pode alugar, arrendar ou emprestar o Software a terceiros.

5.5. Não pode utilizar o Software para criação de dados ou de software utilizado para a detecção, bloqueio ou tratamento das ameaças descritas no Manual do Utilizador.

5.6. O Detentor dos Direitos tem o direito de bloquear o ficheiro da chave ou rescindir a Licença de utilização do Software caso haja alguma violação de qualquer parte dos termos e condições deste Contrato por parte do Utilizador Final sem qualquer reembolso.

5.7. Se o Utilizador Final está a utilizar a versão experimental do Software, não tem o direito de receber a Assistência Técnica especificada na Cláusula 4 deste Contrato e o Utilizador Final não tem o direito de transferir a licença ou os direitos de utilização do Software a terceiros.

6. Garantia limitada e Renúncias

6.1. O Detentor dos Direitos garante que o Software irá cumprir substancialmente o que lhe é devido, de acordo com as especificações e descrições indicadas no Manual do Utilizador *desde que, no entanto,* essa garantia limitada não se aplique ao seguinte: (w) As deficiências e violações relacionadas do computador para as quais o Detentor dos Direitos renuncia expressamente todas as responsabilidades da garantia; (x) avarias, defeitos ou falhas resultantes de má utilização; abuso; acidente; negligência; instalação imprópria, operação ou manutenção; roubo; vandalismo; casos fortuitos; actos de terrorismo; falhas de energia ou picos de potência; acidentes; alterações, modificações não permitidas ou reparações por qualquer parte além do Detentor de Direitos; ou as acções do Utilizador Final ou causas que estejam para além do controlo razoável do Detentor dos Direitos; (y) qualquer defeito que o Utilizador Final não tenha dado a conhecer ao Detentor de Direitos logo que possível depois de o defeito aparecer pela primeira vez; e (z) incompatibilidade provocada pelos componentes de hardware e/ou software instalados no Computador do Utilizador Final.

6.2. O Utilizador Final reconhece, aceita e concorda que não existe nenhum software isento de erros e o Utilizador Final é aconselhado a fazer cópias de segurança do Computador, com a frequência e a fiabilidade adequada para o Utilizador Final.

6.3. O Detentor dos Direitos não oferece qualquer garantia de que o Software irá funcionar correctamente em caso de violações dos termos descritos no Manual do Utilizador ou neste Contrato.

6.4. O Detentor dos Direitos não garante que o Software irá funcionar correctamente se o Utilizador Final não fizer regularmente transferências das Actualizações especificadas na Cláusula 2.5 deste Contrato.

6.5. O Detentor dos Direitos não garante protecção das ameaças descritas no Manual do Utilizador após a expiração do período especificado nas

Cláusulas 3.2 ou 3.3 deste Contrato ou após a rescisão da Licença de utilização do Software, caso ela seja rescindida por qualquer razão.

6.6. O SOFTWARE É ENTREGUE "TAL COMO ESTÁ" E O DETENTOR DOS DIREITOS NÃO FAZ QUALQUER REPRESENTAÇÃO NEM DÁ QUAISQUER GARANTIAS DA SUA UTILIZAÇÃO OU DESEMPENHO. EXCEPTO NO QUE SE REFERE A QUALQUER GARANTIA, CONDIÇÃO, REPRESENTAÇÃO OU TERMO NA MEDIDA EM QUE NÃO POSSA SER EXCLUÍDA OU LIMITADA PELA LEI APLICÁVEL, O DETENTOR DOS DIREITOS E OS SEUS PARCEIROS NÃO CONCEDEM QUALQUER GARANTIA, CONDIÇÃO, REPRESENTAÇÃO OU TERMO (EXPRESSO OU IMPLÍCITO, QUER SEJA POR ESTATUTO, LEI COMUM, PERSONALIZAÇÃO, UTILIZAÇÃO OU QUALQUER OUTRO) QUE, SEM OUTRO ASSUNTO INCLUINDO, MAS NÃO SE LIMITANDO, A NÃO INFRACÇÃO DOS DIREITOS DE TERCEIROS, COMERCIALIZAÇÃO, QUALIDADE SATISFATÓRIA, INTEGRAÇÃO OU APLICABILIDADE A UM FIM ESPECÍFICO. O UTILIZADOR FINAL ASSUME TODAS AS AVARIAS E TODO O RISCO DE DESEMPENHO E RESPONSABILIDADE POR SELECCIONAR O SOFTWARE DE MODO A CONSEGUIR OS RESULTADOS PRETENDIDOS, E PELA INSTALAÇÃO, UTILIZAÇÃO E RESULTADOS OBTIDOS DO SOFTWARE. SEM LIMITAR AS DISPOSIÇÕES ANTERIORES, O DETENTOR DOS DIREITOS NÃO CONCEDE QUALQUER REPRESENTAÇÃO E NÃO DÁ GARANTIAS DE QUE O SOFTWARE NÃO CONTÉM ERROS OU NÃO ESTÁ LIVRE DE INTERRUPÇÕES OU OUTRAS FALHAS OU QUE O SOFTWARE VAI AO ENCONTRO DE TODOS E QUAISQUER REQUISITOS DO UTILIZADOR FINAL TENHAM OU NÃO SIDO DIVULGADOS AO DETENTOR DOS DIREITOS.

7. Exclusão e limitação da responsabilidade

NA MEDIDA MÁXIMA PERMITIDA PELA LEI APLICÁVEL, EM CASO ALGUM O DETENTOR DOS DIREITOS OU OS SEUS PARCEIROS SÃO RESPONSÁVEIS POR QUAISQUER DANOS ESPECIAIS, ACIDENTAIS, PUNITIVOS, INDIRECTOS OU CONSEQUENCIAIS, SEJAM ELES QUAIS FOREM, (INCLUINDO, MAS NÃO SE LIMITANDO A DANOS POR PERDA DE LUCROS OU DE INFORMAÇÕES CONFIDENCIAIS, OU OUTRAS, POR INTERRUPÇÃO DO NEGÓCIO, POR PERDA DE PRIVACIDADE, POR CORRUPÇÃO, DANOS E PERDAS DE DADOS OU PROGRAMAS, POR FALHA DE PAGAMENTO DE QUAISQUER DIREITOS INCLUINDO QUAISQUER DIREITOS LEGAIS, DIREITOS DE LEALDADE OU DIREITOS DE CUIDADOS RAZOÁVEIS, POR NEGLIGÊNCIA, POR PERDA ECONÓMICA, E POR QUALQUER PERDA PECUNIÁRIA OU OUTRA, SEJA ELA QUAL FOR) QUE SURJA DE UMA QUALQUER FORMA RELACIONADA COM A UTILIZAÇÃO OU INCAPACIDADE DE UTILIZAÇÃO DO SOFTWARE, A

DISPOSIÇÃO OU FALHA DE FORNECIMENTO DE ASSISTÊNCIA OU OUTROS SERVIÇOS, INFORMAÇÕES, SOFTWARE E CONTEÚDOS RELACIONADOS ATRAVÉS DO SOFTWARE OU QUE, POR OUTRO LADO, SURJA DA UTILIZAÇÃO DO SOFTWARE, OU, AO CONTRÁRIO, MEDIANTE OU EM LIGAÇÃO A QUALQUER DISPOSIÇÃO DESTE CONTRATO, OU QUE SURJA DE QUALQUER VIOLAÇÃO DO CONTRATO OU QUALQUER DELITO (INCLUINDO NEGLIGÊNCIA, MÁ REPRESENTAÇÃO OU QUALQUER OBRIGAÇÃO OU DEVER DE RESPONSABILIDADE LIMITADA), OU QUALQUER VIOLAÇÃO DOS DEVERES LEGAIS, OU QUALQUER VIOLAÇÃO DA GARANTIA DO DETENTOR DOS DIREITOS OU QUALQUER UM DOS SEUS PARCEIROS, MESMO QUE O DETENTOR DOS DIREITOS OU QUALQUER PARCEIRO TENHA SIDO AVISADO DA POSSIBILIDADE DESSES DANOS.

O UTILIZADOR FINAL CONCORDA QUE, CASO O DETENTOR DOS DIREITOS E/OU OS SEUS PARCEIROS SEJAM TIDOS COMO RESPONSÁVEIS, A RESPONSABILIDADE DO DETENTOR DOS DIREITOS E/OU DOS SEUS PARCEIROS DEVE SER LIMITADA PELOS CUSTOS DO SOFTWARE. EM CASO ALGUM DEVE A RESPONSABILIDADE DO DETENTOR DOS DIREITOS E/OU DOS SEUS PARCEIROS EXCEDER AS TAXAS PAGAS PELO SOFTWARE AO DETENTOR DOS DIREITOS OU AO PARCEIRO (COMO SE APLICAR).

NADA NESTE ACORDO EXCLUI OU LIMITA QUAISQUER REIVINDICAÇÕES DE MORTE E FERIMENTOS PESSOAIS. ALÉM DISSO, NO CASO DE ALGUMA RESPONSABILIDADE, EXCLUSÃO OU LIMITAÇÃO NESTE CONTRATO NÃO POSSAM SER EXCLUÍDAS OU LIMITADAS DE ACORDO COM A LEI APLICÁVEL, ENTÃO APENAS ESSA RESPONSABILIDADE, EXCLUSÃO OU LIMITAÇÃO NÃO SE DEVEM APLICAR AO UTILIZADOR FINAL E CONTINUA A FICAR VINCULADO POR TODAS AS RESTANTES RESPONSABILIDADES, EXCLUSÕES E LIMITAÇÃO.

8. GNU e outras licenças de terceiros

O Software pode incluir alguns programas de software licenciados (ou sublicenciados) ao utilizador no âmbito da Licença Pública Geral GNU (General Public License, GPL) ou outras licenças semelhantes de software grátis que, entre outros direitos, permite ao utilizador copiar, modificar e redistribuir determinados programas, ou partes do mesmo, e ter acesso ao código fonte ("Software de Código Aberto"). Se essas licenças necessitarem que, para qualquer software que é distribuído às pessoas num formato de binário executável, que o código fonte também seja tornado disponível a esses utilizadores, então o código fonte deve ser tornado disponível enviando o pedido para source@kaspersky.com ou é fornecido com o Software. Se quaisquer licenças de Software de Código Aberto precisarem que o Detentor dos Direitos forneça direitos de utilização, cópia ou modificação de um programa de Software

de Código Aberto, mais vastos do que os direitos concedidos neste Contrato, então esses direitos devem ter precedência sobre os direitos e restrições aqui indicados.

9. Posse dos direitos de propriedade

9.1 Concorda que o Software e a respectiva autoria, os sistemas, ideias, métodos de funcionamento, documentação e outras informações contidas no Software, são propriedade intelectual registada e/ou segredo comercial, de grande valor, do Detentor dos Direitos ou dos seus parceiros e que o Detentor dos Direitos e os seus parceiros, conforme aplicável, estão protegidos pela lei civil e criminal e pelas leis de direitos de autor, segredos comerciais, marcas registadas e patentes da Federação Russa, União Europeia e Estados Unidos e de outros países, bem como pelos tratados internacionais. Este Contrato não concede ao Utilizador Final quaisquer direitos no que se refere à propriedade intelectual, incluindo as marcas comerciais ou as marcas dos serviços do Detentor dos Direitos e/ou dos seus parceiros ("Marcas Comerciais"). Pode utilizar as Marcas Comerciais apenas e até ao ponto de identificar resultados impressos produzidos pelo Software de acordo com a prática das marcas comerciais aceites, incluindo a identificação do nome do proprietário da Marca Comercial. A utilização de qualquer Marca Comercial não dá ao Utilizador Final quaisquer direitos de propriedade sobre essa Marca Comercial. O Detentor dos Direitos e/ou os seus parceiros são proprietários e retêm todos os direitos, títulos e interesse no Software e em relação ao mesmo, incluindo, sem limitações, quaisquer correcções de erros, melhoramentos, Actualizações ou outras modificações ao Software, quer sejam feitas pelo Detentor dos Direitos ou por quaisquer terceiros, e todos os direitos sobre direitos de autor, patentes, segredos comerciais, marcas comerciais e outras propriedades intelectuais contidas neste documento. A possessão, instalação ou utilização do Software não lhe transfere qualquer título para a propriedade intelectual no Software e não adquire quaisquer direitos ao Software excepto quando expressamente estipulado neste Contrato. Todas as cópias do Software realizadas nos termos do presente Contrato têm de conter os mesmos avisos de propriedade que aparecem no Software. Excepto como aqui indicado, este Contrato não concede ao Utilizador Final quaisquer direitos de propriedade intelectual sobre o Software e o Utilizador Final reconhece que a Licença, tal como está definida aqui, concedida nos termos deste Contrato, concede apenas o direito de utilização limitada mediante os termos e as condições deste Contrato. O Detentor dos Direitos reserva-se todos os direitos não expressamente concedidos ao Utilizador Final neste Contrato.

9.2 O Utilizador Final reconhece que o código fonte, o código de activação e/ou o ficheiro da chave da licença do Software são propriedade do

Detentor dos Direitos e constituem segredos comerciais do Detentor dos Direitos. Concorda em não modificar, adaptar, traduzir, inverter a engenharia, descompilar, desmontar ou tentar, de qualquer outro modo, descobrir o código fonte do Software seja de que forma for.

9.3 Concorda em não modificar nem alterar o Software seja de que forma for. Não pode remover nem alterar quaisquer avisos de direitos de autor ou outros avisos de propriedade em nenhuma cópia do Software.

10. Lei vigente; arbitragem

Este Contrato é regido, e será interpretado, de acordo com as leis da Federação Russa sem referência a conflitos de regras e princípios legais. Este Contrato não será regido pela Convenção das Nações Unidas referente a Contratos para a Venda Internacional de Bens, a aplicação da qual é expressamente excluída. Qualquer litígio que surja no seguimento da interpretação ou aplicação dos termos deste Contrato ou qualquer infracção ao mesmo, a não ser que se resolva por negociação directa, deverá ser resolvido no Tribunal de Arbitragem Comercial Internacional na Câmara do Comércio e Indústria da Federação Russa em Moscovo, na Federação Russa. Qualquer decisão apresentada pelo árbitro deve ser final e obrigatória para as partes e qualquer julgamento sobre essa decisão de arbitragem pode ser feita cumprir em qualquer tribunal da jurisdição competente. Nada nesta Secção 10 deve impedir que uma Parte procure e obtenha qualquer reparação equitativa de um tribunal da jurisdição competente, quer seja antes, durante ou depois dos processos de arbitragem.

11. Período para interpor acções

Nenhuma acção, independentemente da forma, que surja das transacções nos termos deste Contrato, pode ser trazida aqui por qualquer uma das partes mais de um (1) ano depois da causa da acção ter ocorrido, ou de ter sido descoberta a ocorrência, excepto que uma acção por violação dos direitos de propriedade intelectual seja trazida dentro do período legal máximo aplicável.

12. Contrato completo; redução; sem renúncia

Este Contrato constitui todo o contrato entre o Utilizador Final e o Detentor dos Direitos e substitui quaisquer outros acordos prévios, propostas, comunicações ou publicidade, oral ou escrita, referente ao Software ou ao assunto deste Contrato. O Utilizador Final reconhece que leu este Contrato, compreendeu-o e concorda em estar vinculado pelos seus termos. Se qualquer disposição deste Contrato for indicada por um tribunal de jurisdição competente como sendo inválida, nula ou inexequível por qualquer razão, no todo ou em parte, essa disposição será ainda mais restritamente interpretada de tal forma que será legal e executória, e todo o Contrato não falhará por conta do mesmo e o saldo do Contrato continuará válido e com efeitos até ao máximo permitido por lei ou equidade ao mesmo tempo que preserva, até ao máximo possível, a sua

intenção original. Nenhuma renúncia de nenhuma disposição ou condição aqui indicadas será válida a não ser por escrito e assinada pelo Utilizador Final e um representante autorizado do Detentor dos Direitos desde que nenhuma renúncia de nenhuma infracção de nenhuma disposição deste Contrato constitua uma renúncia de qualquer infracção anterior, concorrente ou subsequente. A não insistência por parte do Detentor dos Direitos no que se refere a fazer valer o desempenho rigoroso de todas as disposições deste Contrato ou nenhum direito deve ser interpretado como sendo uma renúncia de qualquer uma dessas disposições ou direitos.

13. Informações de contacto do Detentor dos Direitos

Se tiver quaisquer dúvidas referentes a este Contrato ou se, por qualquer razão, pretender contactar o Detentor dos Direitos, contacte o nosso Departamento de Apoio ao Cliente em:

Kaspersky Lab ZAO, 10 build. 1 1st Volokolamsky Proezd
Moscovo, 123060
Federação Russa
Tel.: +7-495-797-8700
Fax: +7-495-645-7939
E-mail: info@kaspersky.com
Website: www.kaspersky.com

© 1997-2009 Kaspersky Lab ZAO. Todos os direitos reservados. O Software e toda a documentação que o acompanha têm direitos de autor e estão protegidos pelas leis de direitos de autor e por tratados internacionais de direitos de autor, bem como por outras leis e tratados de propriedade intelectual.